NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SECURITY INFORMATION AND EVENT MANAGEMENT TOOLS AND INSIDER THREAT DETECTION

by

Christopher J. Callahan

September 2013

Thesis Advisor: J.D. Fulp
Co-Advisor: Frank Krautheim

Approved for public release; distribution is unlimited

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
SEP 2013	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Security Information And Event Management Tools And Insider Threat Detection	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School Monterey, CA 93943-5000**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Malicious insider activities on military networks can pose a threat to military operations. Early identification of malicious insiders assists in preventing significant damage and reduces the overall insider threat to military networks. Security Information and Event Management (SIEM) tools can be used to identify potential malicious insider activities. SIEM tools provide the ability to normalize and correlate log data from multiple sources on networks. Personnel background investigations and administrative action information can provide data sources for SIEM tools in order to assist in early identification of the insider threat by correlating this information with the individuals online activities. This thesis provides background information on the components and functionality of SIEM tools, summarizes historic insider threat cases to determine common motivations, provides an overview of military security investigations and administrative actions in order to determine candidate sources for SIEM correlation, and provides an overview of common methods of data exfiltration by malicious insiders. This information is then used to develop an example SIEM architecture that highlights how the military can use a SIEM to identify and prevent potential internal insider threats by correlating an individuals network activities with background investigation and administrative action information.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**101**	

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704–0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2013	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE SECURITY INFORMATION AND EVENT MANAGEMENT TOOLS AND INSIDER THREAT DETECTION		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Christopher J. Callahan			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

Malicious insider activities on military networks can pose a threat to military operations. Early identification of malicious insiders assists in preventing significant damage and reduces the overall insider threat to military networks. Security Information and Event Management (SIEM) tools can be used to identify potential malicious insider activities.

SIEM tools provide the ability to normalize and correlate log data from multiple sources on networks. Personnel background investigations and administrative action information can provide data sources for SIEM tools in order to assist in early identification of the insider threat by correlating this information with the individual's online activities.

This thesis provides background information on the components and functionality of SIEM tools, summarizes historic insider threat cases to determine common motivations, provides an overview of military security investigations and administrative actions in order to determine candidate sources for SIEM correlation, and provides an overview of common methods of data exfiltration by malicious insiders. This information is then used to develop an example SIEM architecture that highlights how the military can use a SIEM to identify and prevent potential internal insider threats by correlating an individual's network activities with background investigation and administrative action information.

14. SUBJECT TERMS Insider Threat, Security Information and Event Management, Personnel Security Investigations			**15. NUMBER OF PAGES** 101
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01–280–5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

SECURITY INFORMATION AND EVENT MANAGEMENT TOOLS AND INSIDER THREAT DETECTION

Christopher J. Callahan
Lieutenant, United States Navy
B.B.A, Gonzaga University

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN CYBER SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
September 2013

Author: Christopher J. Callahan

Approved by: J.D. Fulp
Thesis Advisor

Frank Krautheim
Thesis Co-Advisor

Cynthia Irvine
Chair, Cyber Academic Group

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Malicious insider activities on military networks can pose a threat to military operations. Early identification of malicious insiders assists in preventing significant damage and reduces the overall insider threat to military networks. Security Information and Event Management (SIEM) tools can be used to identify potential malicious insider activities.

SIEM tools provide the ability to normalize and correlate log data from multiple sources on networks. Personnel background investigations and administrative action information can provide data sources for SIEM tools in order to assist in early identification of the insider threat by correlating this information with the individual's online activities.

This thesis provides background information on the components and functionality of SIEM tools, summarizes historic insider threat cases to determine common motivations, provides an overview of military security investigations and administrative actions in order to determine candidate sources for SIEM correlation, and provides an overview of common methods of data exfiltration by malicious insiders. This information is then used to develop an example SIEM architecture that highlights how the military can use a SIEM to identify and prevent potential internal insider threats by correlating an individual's network activities with background investigation and administrative action information.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACES	Automated Continuous Evaluation System
CI	Counterintelligence
DISS	Defense Information System for Security
DoD	Department of Defense
DON	Department of the Navy
DONCAF	Department of the Navy Clearance Adjudication Facility
ISCM	Information Systems Continuous Monitoring
JPAS	Joint Personnel Adjudication System
NJP	Nonjudicial Punishment
SAAR-N	System Authorization Access Request-Navy
SEM	Security Event Management
SIEM	Security Information and Event Management
SIM	Security Information Management
TTL	Time To Live
PERSEREC	Defense Personnel Security Research Center
PSI	Personnel Security Investigation

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank both my advisors for their fantastic guidance and assistance throughout this project. Additionally, I owe much to my cyber teammates for all their support throughout the course of this curriculum.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

Computer networks continue to evolve and increase in complexity. As more and more devices are developed with network connectivity capabilities, the surface area for potential security vulnerabilities to these networks and their numerous connected devices increases. Thus, safeguarding networks and the data that transits through them is a perpetual arms race. As new vulnerabilities are discovered, new patches are added; only to be made irrelevant by new vulnerability discoveries, new devices (with new vulnerabilities), new network paths (connected to new devices), or some combination thereof. However, despite the increased complexity and potential vulnerabilities, systems that are properly patched and managed following the "least privilege" principle fair far better when subjected to various attacks.

The insider threat is considered by many to be the most difficult threat to prevent and discover. The insider, by "definition," has authorized access to systems that an outsider will not. The insider is a trusted agent with knowledge that can be leveraged to exploit a system. Much research and many studies have been conducted to try and discover ways to prevent, detect, and mitigate insider threats. The ability of a network administrator to monitor and audit device logs can potentially lead to the discovery of illicit insider activity; or perhaps to indicators that an insider is "about to go rogue." However, given the number of devices connected to a network, the number of employees, the number of potential insider threats, and the time and labor required to properly and thoroughly investigate logs both in real time and historically, such monitoring becomes an overwhelming challenge.

B. OBJECTIVES

The introduction of a technological solution can assist with the goal of more thorough log monitoring. A Security Information and Event Management (SIEM) tool provides a way for system log information from numerous logging nodes to be collected centrally and analyzed for anomalies. If an anomaly is detected, based on the

organization's previously defined rule sets, an alert can be sent to designated security personnel for further investigation or action, if necessary. However, without a properly defined rule-set, the organization runs the risk of having too many false negatives (real threats that are missed) or, conversely, false positives (innocuous events which are erroneously tagged as malicious); exacerbating the defender's job, rather than helping.

Identification of users who may have an increased propensity to conduct illicit activities as insider threat, would be highly beneficial. This could potentially be achieved by focusing a SIEM tool in a manner that reduces false alerts, and more reliably detects malicious insider actions, or perhaps provides indications and warnings that a trusted insider may be in the early planning stages of carrying out some malicious act (Hanley & Montelibano, 2011).

The Department of the Navy (DON) attempts to reduce insider threats by first conducting a background investigation prior to an employee receiving a security clearance and/or network and system access (Secretary of the Navy, 2006). This investigation, called a Personnel Security Investigation (PSI), contains many data points that are not necessarily preclusive of receiving a security clearance or employment within the DON. For example, an employee who may have had financial difficulties in the past but does not have other risky data points in their background investigation, may have no problem receiving a security clearance or system access. However, the fact the employee *had* previous financial difficulties suggests he/she may be more at risk of *becoming* an insider threat at some point in the future.

In addition, administrative actions conducted against an employee for work incidents (poor performance, behavior issues, physical fitness test failures, etc.) can also provide further data points regarding an individual and the risk of insider threats (CERT, 2011). While one or many of these examples may not be indicative or predictive, it can be helpful to have these data points attached to a person's user profile on a network. With these data points accessible, rules can be developed within a SIEM that leverage this additional information in order to more reliably alert on certain network behaviors.

By adding potential security flags already gathered through the process of PSIs and administrative actions, a user's network account can be flagged for monitoring of potentially suspicious or dangerous network behavior. For example, if a user has previously had financial issues, their Web activity could be flagged to issue an alert if they are visiting bankruptcy information or credit counseling sites. While not necessarily predictive of the evolution of an actual insider threat, the alerts can trigger management action which might involve further monitoring, counseling with the individual, or other managerial activities that would ideally prevent the insider from ever getting to the point of actually conducting illegal or malicious activities.

An example SIEM architecture will be designed using ArcSight Express and reviewed for potential applicability to a Navy command in order to address the issues of the insider threat. This architecture will include employee PSI and administrative action data, and represent an attempt at designing a method to relate this data with employee network activities; with the end goal of identifying potential or actual malicious insider activity.

C. ORGANIZATION

This documented is organized into the following chapters:

Chapter II provides background of the origins of SIEM tools, and basics on the dangers of the insider threat.

Chapter III provides details on the basic features of a SIEM. Node logging, normalization, and correlation processes are discussed, and the basic components of a SIEM tool are described. The potential advantages and disadvantages of a SIEM tool are also provided.

Chapter IV contains insider threat definitions and policies. It also contains descriptions of the various categories of insider threats and some of the motivations for insiders conducting malicious activities.

Chapter V is divided into three main parts, PSI, administrative action, and the individual account creation process within the Navy. PSI describes the background

investigations required for military personnel and the process required. The administrative action section describes some of the types of tools available to a command for discipline in response to certain employee activities, and how those actions are documented in the individual's record. The third section describes the process by which an individual obtains a network account within the Navy, and how that might be adjusted in order to include PSI and administrative action items.

Chapter VI describes some of the basic methods an individual can employ to remove information, without authorization, from a command. Some of these described methods can then be incorporated as conditions for the example SIEM architecture.

Chapter VII contains an example SIEM architecture for including PSI and administrative action items. Goals of the SIEM architecture are described and the overall architecture is presented. This description includes the types of filters necessary, the use of multiple active lists, and how the described rules use these active lists. Examples of each, created within ArcSight Express, are provided.

Chapter VIII provides concluding statements regarding the previous chapters, and provides areas that might benefit from additional research leading to a more optimal implementation of a SIEM tool in addressing insider threats.

II. BACKGROUND

A. INFORMATION SYSTEMS CONTINUOUS MONITORING (NIST SP 800–137)

The National Institute for Standards and Technology, under the Federal Information Security Management Act (FISMA), is responsible for development of information security standards and guidelines for federal information systems (Dempsey et al., 2011). As part of these responsibilities, NIST has issued the Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations in September 2011. This publication describes the implementation of ISCM in federal organizations as part of an overall risk mitigation and management strategy for federal information systems.

Previous federal publications highlighted the importance of monitoring information systems as part of the overall management of security practices. However, these methods of monitoring information systems were manpower intensive. There are now automated tools available that assist managers in their ability to conduct continuous monitoring of their information systems, traffic, and users' network activities in order to better provide effective security controls from both inside and outside threats. NIST describes the goal of these automated monitoring tools as being able to be "readily deployed in support of near real-time, risk-based decision making" (Dempsey et al., 2011, p. 8).

NIST defines ISCM as an organization maintaining ongoing awareness of information security vulnerabilities and threats to support organizational risk management decisions. It further elaborates on the ISCM program and process where the program is "established to collect information in accordance with pre-established metrics, utilizing information readily available in part through implemented security controls" (Dempsey et al., 2011, p. vii). The overall ISCM process contains the key elements of analyzing the data, reporting the findings, and responding to those findings (Dempsey et al., 2011). This analysis of data and reporting of the results can be assisted through the use of an automated security tool such as a SIEM product.

NIST defines SIEM tools as being able to "enhance the ability to identify inappropriate or unusual activity…through analysis of vulnerability scanning information, performance data, network monitoring, and system audit record (log) information" (Dempsey et al., 2011, p. D-10). A SIEM is basically a tool that can receive inputs from multiple nodes that may be manufactured by multiple vendors, filter for select information, normalize these inputs, aggregate the inputs as necessary, and then conduct rule-based analysis on the inputs in order to detect patterns or anomalies that may require further action by management personnel.

B. SIEM ORIGINS

The advancement of technologies has allowed for the development of these SIEM tools that can provide an organization's management with a continuous monitoring solution for a variety of their information system needs, including those described in the NIST SP 800–137. The emergence of the SIEM as a multi-task capable tool has provided organizations with the capability to manage and monitor network data that was previously difficult due to both the vast amount of data, and the dearth of technically capable personnel available to conduct the analysis.

The origin of the acronym SIEM comes from the combination of Security Information Management (SIM) and Security Event Management (SEM). SIM tools aggregated and stored log data for organizations. SEM tools applied some sort of analysis to this log data in order to assist in identifying potential threats. The combination of these two related capabilities produced the modern SIEM (Schultz, 2009). These tools are also sometimes referred to as Enterprise Security Management (ESM) (Contos, 2006). Throughout this paper, these tools will be referred to as SIEM tools. These early SIEMs emerged to assist network security personnel in filtering through firewall data, intrusion detection data, router events, etc., in order to eliminate false positives and identify true threats (Sensage, n.d.).

C. INSIDER THREAT DANGERS

Recent events highlighting the dangers of insider threats such as Army PFC Bradley Manning and others have reinforced the need for more accurate means and methods to assist in the identification of insider threats. While Bradley Manning caused much of the damage from his alleged access to a classified network and subsequent release of hundreds of thousands of classified documents (Weiss, 2013), insiders can still cause damage with only unclassified access. The DoD has obvious concerns over the control of unclassified information and has released a directive, DODM 5200.01-V4, defining specific requirements for managing Controlled Unclassified Information (CUI). A malicious insider can cause considerable damage regardless of the classification of the networks compromised.

Early detection of these events can decrease the amount of damage resulting from malicious insider activities. Insiders have an obvious attack advantage, as they will likely have significant "insider" information on the organization to which they are attached. This allows them greater freedom of movement within the organization and a reduced threat of detection if they know the security policies and procedures of the organization to which they are attached. It is also easier for an insider to explain away potentially malicious behavior as owing to ignorance or accidental violations. Monitoring an insider's activities on an organization's network, classified or unclassified, offers the possibility of earlier detection, and perhaps even prevention, of malicious activities. A SIEM can assist in identifying and correlating these activities. A SIEM can also be used to focus on personnel who may have factors in their background that might increase their overall security risk.

THIS PAGE INTENTIONALLY LEFT BLANK

III. SIEM CAPABILITIES

A. SIEM BASIC FEATURES

According to research conducted by the Gartner group, SIEMs are typically employed by corporations for use against internal and external threats, monitoring user activities, monitoring servers and databases, and for rules and regulation compliance (Nicolett & Kavanagh, 2012). The general functions and features of SIEMs are highlighted below in order to illustrate the capabilities of these tools.

1. Node Logging

Each network can be unique to an organization. While headquarters may set configuration policies regarding basic design and topology, there are many variations that can occur within a specific network, even amongst similar organizations or departments. There are many types of nodes on these networks that can provide logs or information for SIEM collection. Some examples include printers, servers, and door key access logs, alarm activation logs, and applications such as web-browsing or e-mail. These nodes can be capable of producing logs detailing a variety of activities related to the specific node. Some typical types of event logs are operations performed by the node, times of operations, personnel who accessed the node, personnel who initiated the operation, and others depending on the type of node. These logs provide records of activities that can be potentially collected and analyzed using a SIEM tool (Schultz, 2009).

2. Event Normalization

Prior to collecting the logs from various node sources, there must be a way to translate the various formats of these devices and applications into a common format. “When events from heterogeneous sources are normalized, they can be analyzed by a smaller number of correlation rules, which reduces deployment and support labor. In addition, normalized events are easier to work with when developing reports and dashboards” (Nicolett & Kavanagh, 2012). There are two widely used formats for normalizing these log events. One is the Common Event Expression, which was

developed by the MITRE Corporation, and the other is Common Event Format, developed by ArcSight (Capelli, Moore, & Trzeciak, 2012).

3. Correlation

After normalizing the log events for central collection and analysis, there must also be a way to correlate the events with each other. This correlation can be between events from the same source or from different sources. Manually correlating numerous logs can be a difficult process as the amount of data events produced from even a single node can yield vast amounts of information. This can create a situation where it is not realistic to manually analyze and correlate these events and potential indicators of malicious activities may go undetected. A SIEM provides a means to apply pre-defined rules automatically to the collected, aggregated and normalized events. This removes the requirement for personnel to manually analyze events. A SIEM rule can be defined to indicate a correlation if certain log event parameters are met. These rules can be designed to highlight a correlation between events that may indicate malicious insider activity (ArcSight, 2012).

For example, a log event may be generated showing an employee accessing a station or office outside of normal work hours for that specific employee (Capelli et al., 2012). In addition, log events may be generated showing a high level of printer activity from that employee's workstation. Any or all employee actions that elicited these events may be benign, or they may be indicative of malicious activity. By correlating the events, a deeper picture of that employee's overall network activities can be derived, and potential issues may be identified for further investigation.

The employee may simply be working after hours to finish legitimate work requirements. The employee may be exploiting the organization's availability of free printing services for non-work related activities. Or, more dangerously, the employee may be attempting to remove sensitive data during hours when fewer people will question or observe these activities. In any case, these two individual events, when correlated, might trigger an alert for that employee's supervisor for more detailed investigations or actions (Schultz, 2009). Using a SIEM's capability to automatically

correlate events based on applied rules can provide insight into potentially related activities of interest that may require further evaluation or investigation (Capelli et al., 2012).

4. Filters

With numerous nodes providing log events, it becomes necessary to filter out some log event inputs and concentrate on the important events. *Important*, in this context, means those events that are deemed most likely to provide meaningful security cueing information. Filters are used to reduce the overall amount of events processed by the SIEM. Filters can be designed to be broad or narrow in the scope of events they filter. For example, an administrator may wish to only include log events from certain workstations or IP addresses, or during a specific time period, or even certain applications involved. Filters can be specified to focus on these events for evaluation and they can also be used as components of a SIEM rule. Within the ArcSight SIEM product, filters are a basic component used in rule development. They are a "set of conditions that focus on particular event attributes" (ArcSight, 2012, p. 57). The filters select only the events that match those conditions for further processing by the SIEM. A filter is defined using ArcSight's Common Conditions Editor, and once defined it can be saved as a *named conditions filter* that allows it to be used by other resources of the SIEM (ArcSight, 2012). Rules can then easily implement those named condition filters as components of the overall rule without having to define the same filter over and over. This can also help limit mistakes in rule development if a filter is rather complex (Miller, Harris, Harper, VanDyke, & Blask, 2011).

5. Rules

Rules are used within a SIEM to evaluate events received from normalized log data that will produce a certain result. Rules within ArcSight are typically created using a combination of previously defined filters "joined together" using Boolean logic (e.g., AND, OR, NOT). The intent is to design rules to perform some useful security action when the semantics of some select subset of events collectively indicate the existence, or possibility of existence, of a security policy violation. Aggregation within rules allows for

for responses to be triggered after a specified number of occurrences within a specified time frame. This can be useful in recognizing patterns of activities and can also reduce false positives based on single occurrence events. Rules within ArcSight can be configured to take one or more actions based on one event, multiple events, event thresholds, or some minimum number of events occurring within some specified time interval(s) (Miller et al., 2011).

When the previously defined conditions of a rule are met within ArcSight, a correlation event occurs and is added to the database, highlighting the important event for SIEM operators (ArcSight, 2012). In addition to generating correlation events, matched rules can also perform previously defined actions. Two example actions are: 1) sending notifications to designated personnel, and 2) executing a mitigating response action such as shutting down an infected node (Miller et al., 2011). Further details of designing SIEM rules used within ArcSight will be examined in Chapter VII.

6. Dashboards

The use of dashboards within SIEMs allows for a convenient central location for monitoring an organization's network activity. The various logs from nodes connected to the SIEM can be used as data sources for display on the dashboard. The dashboard may be configured to display a variety of information related to the dashboard monitor's advertised usage and functionality, or some other tailor-made information that supports the unique needs of an organization. If an item of interest or an alert shows up on a SIEM dashboard, the SIEM operator interface allows the operator to drill-down on the information regarding the event in order to more closely inspect and analyze the activity (ArcSight, 2012).

7. Alerts and Reports

Data from the various events and activities that provide log event sources to the SIEM can be used to generate alerts and reports. Depending on the event and the rules established for that event, an alert may be sent to a supervisor or to a security specialist within the organization. These alerts are preconfigured so they are generated automatically when a trigger event or event threshold occurs that warrants an alert. Also,

reports can be generated within a SIEM that can show a variety of data germane to a given incident or case. These reports can be generated on a set cycle or as needed, depending on the situation and needs of the organization. Reports can be used to assist in evaluating events in more detail or by comparing events to historic data (ArcSight, 2012).

8. Log Storage

One crucial configuration parameter relates to log storage. An organization must typically comply with a variety of regulations and policies (both organization specific and legal imperatives) regarding the storage of its log records. In the initial set-up of the SIEM (and periodically as well), an organization can designate priority records for log storage in terms of its size limits and time limits in order to comply with pertinent regulations (Schultz, 2009). This storage will also affect the ability to correlate events as significant time may elapse between important network events. This might result in a failure to detect a slowly evolving attack. For example, if an event drops out of the database due to expired time, another similar event will not be considered quite as serious during correlation by the SIEM as there were no pre-existing events to show a potential pattern.

B. SIEM ADVANTAGES AND DISADVANTAGES

As with any tool, there are certain advantages and disadvantages associated with SIEM implementation, operation, and maintenance that will affect its utility to the organization and its overall performance. The following sections highlight some of the general advantages and disadvantages with SIEM usage. A SIEM will have different values to an organization depending on the desired features and accessories available.

1. SIEM Advantages

In addition to the reasons provided above highlighting the capabilities of a SIEM tool and the advantages of its use, a properly configured and implemented SIEM can also provide for an overall reduction in labor time and costs. A SIEM's ability to consolidate multiple logs from multiple products into a central location, while automatically checking events against previously defined rules, will greatly decrease the amount of time required

compared with that required for one or more analysts to perform these functions manually. A SIEM's ability to centrally manage multiple resources while filtering events and conducting analysis and then automatically generating reports and alerts can significantly improve the security posture of an organization's network. However, it is difficult to put a dollar amount to the value of an improved security posture, as the costs of defending against unrealized threats are not easily quantifiable (Schultz, 2009).

2. SIEM Disadvantages

The overall monetary costs and time costs of installing and maintaining useful technology can be prohibitively expensive for some organizations. Depending on the organization's requirements, these costs can effectively prevent that organization from taking advantage of the previously described benefits of SIEM tools. The costs to consider for a SIEM generally include purchase, installation, maintenance, employee training and ongoing licensing, depending on the size and scale of SIEM required.

The dollar amount for a SIEM can be fairly easy to ascertain based on the vendor's sales information. However, the cost that is difficult to estimate is the cost and labor lost due to the installation of the system: "…installation for such SIEM tools may take up to an entire month" (Schultz, 2009, p. 7). This installation process can have a severe negative impact for an organization's functionality as network nodes are connected and their output fed into the centralized SIEM system. There can also be significant ongoing costs related to allocating staff time for SIEM operations and maintenance.

a. Operations

In order for a SIEM to be of maximal use to an organization; it must be in continuous and constant operation. This can be a potential downside to a SIEM if an organization has difficulty maintaining the constancy of SIEM operations. Also, the required integration of the numerous nodes into the SIEM can be a difficult managerial and technical problem. After a SIEM is up and smoothly running, updates present an ongoing challenge. Software updates for the SIEM software, updates for the connected

nodes, and hardware updates will present added challenges for integration for network administrators (Schultz, 2009).

b. False Security

Another potential disadvantage to using a SIEM is the false sense of security that may develop within an organization. If a SIEM is operating and everything appears to be normal for the SIEM operators, the operators may become lulled into believing everything is well with the network. SIEM operators must ensure there is a process for checking the SIEM to ensure it is correctly operating: nodes are connected, logs are being collected, correlated, and managed, and rules and dashboards are accurately displaying the desired information. The potential complexity of a SIEM can result in the possibility where disconnected or misconnected nodes might spiral into catastrophic network failures, or situations where serious network events are ignored (Schultz, 2009).

c. Data Storage

As technology develops, components on networks are able to generate logs of operations, user actions, maintenance requirements, and a variety of other types of data. This data can be collected and analyzed by the SIEM in order to monitor for potential items of interest. However, as there is more and more data available for a SIEM to collect, analyze, and archive, the requirement for data storage also increases. An organization must ensure it is collecting and storing the data to meet its requirements as defined by the organization. If an organization's data storage capacity is overwhelmed, new data may be lost or otherwise not available for analysis, and the SIEM will no longer function properly (Schultz, 2009).

The availability of a node to provide data to a SIEM does not necessarily mean that *all* the data that *could* be collected, *should* be collected (Schultz, 2009). Balancing the needs of the organization against the capabilities of the SIEM, the network, and the storage capacity of the organization, will be necessary to achieve optimum functionality of the SIEM in its ability to provide defense against the insider threat.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. INSIDER THREATS

The purpose of this paper is to explore the feasibility of using a SIEM's capabilities together with data collected and readily available on military personnel, both officers and enlisted, in order to *deter*, potentially *prevent* and—at a minimum--hopefully *detect* insider threats. Like any other organization, the military is susceptible to insider threats and the mitigation of the insider threat is critical to the military's mission. However, if it is impossible to *prevent* the threat, then *detecting* insider threat activity at the earliest possible moment is the next goal in order to limit the damage. Further, simple awareness that a threat detection capability is in place may *deter* the insider from even considering any threat actions, owing to the increased risk of detection and punishment. The military must also adhere to national policy and service policy in order to remain in compliance with instructions dictating the need to combat the insider threat.

Insider threats in the private sector can use the same tactics, techniques, and procedures as those within the military. These private sector insider threats will likely have the same motives, profiles, and characteristics as those within the military. This chapter will explore insider threat definitions and policies, historic data on insider threat events, and historic data on insider threat motivations. The goal is to develop potential profiles or possible indicators for insider threats. This data can then be used to construct SIEM rules for an individual's specific activity within a network, with the goal of malicious insider detection.

A. INSIDER THREAT DEFINITIONS AND POLICIES

There are recent policies and instructions released by the President of the United States and DoD concerning insider threats within the United States government. These documents contain information to assist in combatting the insider threat as well as definitions of the insider threat. This section will examine DoD definitions of insider threats, the recent presidential memorandum regarding insider threats, and the DoD instruction related to insider threat programs.

1. DoD Definitions

a. Insider

DoD defines an insider as "anyone who has authorized access to DoD resources by virtue of employment, volunteer activities, or contractual relationship with DoD" (Under Secretary of Defense [I], 2012).

b. Insider Threat

DoD defines the insider threat as "a person with authorized access, who uses that access, wittingly or unwittingly, to harm national security interests or national security through unauthorized disclosure, data modification, espionage, terrorism, or kinetic actions resulting in loss or degradation of resources or capabilities" (Under Secretary of Defense [I], 2012).

2. National Insider Threat Policy Presidential Memorandum November 21, 2012

This brief memorandum outlines the basic requirements for government departments to combat the threat from insiders. This memorandum requires departments to "deter, detect, and mitigate actions by employees who may represent a threat to national security" (White House, 2012), which is the goal of this research, specifically for Navy military members. In addition, the memorandum dictates the requirement to have the "capability to gather, integrate, and centrally analyze and respond to key [insider] threat related information" (White House, 2012). This requirement can be aided in execution by a SIEM via its capability to incorporate employee data into its rules and analytical procedures.

3. DODI 5240.26 Countering Espionage, International Terrorism, and the Counterintelligence Insider Threat

This instruction "establishes policy, assigns responsibilities, and provides procedures for counterintelligence (CI) activities to counter espionage and international terrorist threats to DoD…" (Under Secretary of Defense [I], 2012). Within Enclosure 2 of this instruction is the direction of responsibilities of the secretaries of the military

departments. One of these instructions is for the department secretaries to "establish and implement CI initiatives to identify and counter espionage, international terrorism, and the CI insider threat." (Under Secretary of Defense [I], 2012). Incorporating a SIEM with rules based on users' PSI and adverse administrative action data, as part of a department's insider threat detection capability could assist in meeting the objectives of this instruction. Another relevant item is for the secretaries to "conduct anomaly based detection activities..." (Under Secretary of Defense [I], 2012). Again, the use of a SIEM can assist in meeting this requirement through event correlation rules designed to detect anomalous activities.

4. DoD Counterintelligence Insider Threat Program

Within DODI 5240.26 is Enclosure 3, which contains requirements for the establishment of a Counterintelligence (CI) Insider Threat Program. Items from this program that are most relevant to this thesis are described below.

a. Auditing and Monitoring

The first element of the program includes the directive to conduct on-line behavioral monitoring. This must be done with a set of automated tools that will have the ability to easily share data across the DoD and the Intelligence community to ease interoperability within DoD and the IC (Under Secretary of Defense [I], 2012). Tailoring rules to each user for specific monitoring and being able to easily share this information across DoD and Intelligence Community systems is key for this tool to function effectively. Without the sharing capability, crucial data could be lost and not travel with the employee as they move from command to command.

b. Analyzing Foreign Influence

The second item addresses the requirement for a process in which DoD personnel can report all their foreign travel and foreign contacts. This element states the process shall be integrated into the travel system and that both pre-travel and post-travel briefings are required (Under Secretary of Defense [I], 2012). This requirement is an attempt to document an employee's potential foreign influence. An employee who travels

to foreign countries may be susceptible to recruitment efforts by foreign intelligence actors or may develop sympathies to those countries. Also, an employee who has close and continuing contact with foreigners may also be susceptible to recruitment, or influence, by those foreigners. This requirement for reporting foreign influence can become an integral part of a specific user's account.

c. PSI Requirements

This item directs the program to comply with all the requirements in the DoD Manual 5200.01-V-3, the DoD Information Security Program: Protection of Classified Information. If, during the course of a PSI, potential CI information becomes available regarding an individual, both the personnel security and the CI professionals must coordinate their activities (Under Secretary of Defense [I], 2012). This item also directs these entities to coordinate if CI information comes to light during personnel evaluations, analysis and reporting. It is required for personnel with security clearances to report to their security representative a variety of potential CI related incidents. This is required because these incidents can potentially make an individual more susceptible to becoming a malicious insider. These events are then evaluated in order to determine if the individual will maintain their clearance. These events, by themselves and depending on their severity, may not prevent employment or network access. The security evaluation process considers the overall trustworthiness of the person as a whole and granting a clearance is not necessarily determined by a single/isolated event. However, if a person receives and maintains a security clearance despite any reported or discovered issues, a SIEM can use these events and attach these potential security flags to a user.

d. Incident Reporting

This element also requires both CI and security professionals to coordinate their activities and efforts in order to "obtain records of security incidents, violations, suspicious incidents, and anomalies by DoD affiliated persons…" (Under Secretary of Defense [I], 2012). These items can also be used to tailor a SIEM rule to a specific user.

e. Information Assurance

The previous elements stressed the importance of both CI professionals and personnel security professionals working together to combat the insider threat as part of the overall insider threat program. It is at this point that the document describes the need for CI, Security, Information Assurance, and Anti-terrorism/Force Protection personnel to share the responsibility for the mission of countering insider threats specifically related to CI (Under Secretary of Defense, 2012). This need is highly relevant to the goals of this paper. The overall objective is to integrate Personnel Security Investigations, potentially adverse administrative information, and other potential insider threat indicators into a profile for a user that can be used by a SIEM. Coordination and communication between the various personnel responsible for these items is necessary for this to work effectively.

The previously described policies and definitions concerning insider threats will be used throughout this paper. In Chapter VII, sample SIEM rules tailored to user profiles will be used to demonstrate potential fulfillment of these policies and instructions. In order to better tailor these sample SIEM rules, we examine historical insider threats in an attempt to identify potential indicators for insider threats. The following section reviews historical insider threats within both the government and commercial sectors.

B. INSIDER THREAT CATEGORIES

Many organizations have conducted research into the insider threat and produced reports with their findings. One report the DoD produced is the *DoD Insider Threat Mitigation Report*. This report is dated from April 2000, but is still practical owing to its use of historic cases. The goal of the report is to "mitigate the insider threat to DoD information systems" (Information Assurance Technology Analysis Center, 2000, p. i). Some of the key findings of this report include the need to "strengthen personnel security and management practices,…detect problems,…and react/respond" (Information Assurance Technology Analysis Center, 2000, p. i).

The following section examines the four categories of insider threats as described in this report as well as their comparable definitions from the CERT Insider Threat Center. The CERT Insider Threat Center is part of the Software Engineering Institute located at Carnegie Mellon University. It is a research and development organization that receives funding from the U.S government. Its stated objective is to "assist organizations in preventing, detecting, and responding to insider compromises" (Capelli, et al., 2012). As part of its insider threat research, the CERT Insider Threat Center has conducted numerous studies and analyses of historic insider threat cases.

1. Maliciousness and Intentional Abuse

Maliciousness is described as an insider threat source "that results in compromise or destruction of information, or disruption of services to other insiders" (Information Assurance Technology Analysis Center, 2000, p. 6). This can be understood to be an intentional act by a person with knowledge of what the results of their acts will be. This person intends to cause these acts and conducts his activities to achieve these goals. This description is comparable to CERT's intentional abuse insider threat category (Capelli et al., 2012).

2. Disregard of Security Practices and Failure to Adhere to Policies

For this definition, the compromise or destruction of information is a result of disregarding security practices and policies. Some examples include willfully storing classified information improperly, transmitting classified information improperly, and not providing required protection and control for classified information outside of controlled areas (Information Assurance Technology Analysis Center, 2000). The user in these examples may not have malicious intent, and any infraction may be the result of simple laziness rather than willful malice. But the end result is still that sensitive information could be compromised. The user has knowledge of the required security practices but actively chooses to not comply with those practices. This description is comparable to CERT's description of the "failure to adhere to policies" category of insider threats (Capelli et al., 2012)

3. Carelessness and Unintentional Abuse

Being careless with security procedures is a clear path to compromising information. This category from the DoD Insider Threat Mitigation report is comparable with CERT's classification of unintentional abuse as an insider threat (Capelli et al., 2012). The user did not intend to cause damage; but damage was caused. In the DoD sense of damage, carelessness as a source of insider threats generally, but not always, results in minimal damage (Information Assurance Technology Analysis Center, 2012).

4. Ignorance and Unintentional Abuse

For the "ignorance" category, the user was not being malicious, not willfully ignoring security practices, and not being careless with known security practices. The user simply did not *know* the applicable proper security practices and requirements. This can also be compared to CERT's unintentional abuse classification (Capelli et al., 2012).

This paper will focus on the first of these four insider threat categories: "maliciousness and intentional abuse" as described by CERT and DoD. While the other categories of insider threats can cause significant damage to an organization, or result in the compromise of critical information; there is an extra layer of difficulty in attempting to implement a correlation tool that can predict a user's carelessness or ignorance and the likelihood of those characteristics progressing into a *malicious* insider threat type of situation.

C. INSIDER THREAT MOTIVATIONS

This section will examine the insider threat studies conducted by the Defense Personnel Security Research Center and the research studies conducted by CERT. The results will be summarized and examined in order to attempt to determine potential factors related to malicious and intentional abuse motivations that would be good candidates for incorporation into a SIEM rule.

1. Defense Personnel Security Research Center

The Defense Personnel Security Research Center (PERSEREC) is a component of DoD. This organization produces a variety of products and reports related to DoD security clearance programs. The most significant two reports for the purpose of this paper are PERSEREC's "Espionage and Other Compromises of National Security" and "Changes in Espionage by Americans: 1947–2007."

a. Espionage and Other Compromises of National Security

The relevant results of this summary by PERSEREC show that the majority of the espionage cases were insiders and not external foreign agents (Defense Personnel Security Research Center, 2009).

b. Changes in Espionage by Americans: 1947–2007

This PERSEREC report specifically addresses the summary of insider threat data from 1947 through 2007. Its purpose is to show the changes in multiple factors related to American espionage from 1947 through 2007. The report breaks up the years analyzed into 1947 to 1979, 1980 to 1989, and events since 1990 (Herbig, 2007). The report provides multiple sources of data analysis that will be useful for attempting to discover factors or data that might be utilized by a SIEM rule for correlation and analysis. Table 1 shows a breakout of insider motivations separated by each of the three previously defined year groups.

Characteristics	1947-1979		1980-1989		1990-2007	
	n	%	*n*	%	*n*	%
Money						
Sole motive	20	47	26	74	1	7
Primary among multiple motives	10	43	21	60	9	39
Divided loyalties						
Sole motive	7	16	4	11	8	57
Primary among multiple motives	6	27	5	14	9	39
Disgruntlement						
Sole motive	7	16	2	6	3	22
Primary among multiple motives	5	22	3	9	3	13
Ingratiation						
Sole motive	4	9	1	3	2	14
Primary among multiple motives	1	4	6	17	2	9
Coercion						
Sole motive	4	9	0	0	0	0
Primary among multiple motives	1	4	0	0	0	0
Thrills						
Sole motive	1	3	1	3	0	0
Primary among multiple motives	0	0	0	0	0	0
Recognition or ego						
Sole motive	0	0	1	3	0	0
Primary among multiple motives	0	0	0	0	0	0

Table 1. Motivations for Individuals for Espionage (From Herbig, 2009, p. 32)

Table 1 shows the clear leader in motivations for personnel conducting espionage from 1990 to 2007 is divided loyalties. Divided loyalties is defined by Herbig as "an allegiance to another country or cause in addition to the United States, a preference for interests other than the United States, and the possibility for the betrayal of American interests that divided loyalties could cause" (Herbig, 2009, p. 11). Divided loyalties are such an important potential risk factor that they are addressed during an employee's PSI in four sections. These sections are "allegiance to the United States, foreign influence, foreign preference, and outside activities" (Herbig, 2009, p. 12).

For the year group 1990 to 2007, of the 17 events identified as being motivated by divided loyalties, eight had divided loyalties as the sole motive. The proportion of events motivated by divided loyalties for which divided loyalties was the

sole motivation has increased over the years. . Interestingly, motivations due to money as the only motive appear to be declining in recent years; but motivations with money as the primary motive among other motives is still high.

In addition to money and divided loyalties, the other significant motivators are employee disgruntlement and ingratiation. Disgruntlement is defined as "usually being caused by the person's relationships or treatment in the workplace, and the associated desire to take revenge" (Herbig, 2009, p. 35). Ingratiation is the employee's desire to increase their status in the eyes of their "spouse or other family member, a friend, or a handler…" (Herbig, 2009, p. 36).

Based on Table 1's summary of historic espionage data, extra (focused) consideration should be given to divided loyalties, financial considerations, and disgruntlement or ingratiation as potential motivators for insider threats. These factors are potentially identifiable elements that could be used to develop event inputs to rules for SIEM correlation and analysis. Foreign influence and financial issues can be discovered through background investigations during a PSI. Disgruntlement can potentially be discovered during a PSI with investigations of previous supervisors as well as with records of adverse administrative actions. However, the ability to identify an insider motivated by ingratiation—the desire to increase their status in the opinion of others—might be difficult to assess based on PSI's or administrative actions, and will thus not be included as a targeted behavior/metric for SIEM insider threat cueing.

2. CERT/Secret Service Insider Threat Studies

CERT and the United States Secret Service have collaborated to produce reports concerning the insider threat. Several of their reports are highlighted and summarized in this section. The sectors focused on in these CERT reports concerning the insider threat are critical infrastructure, banking and finance, information technology and communications, and government.

These reports were released over a several year period and the summaries below are taken from the research summaries presented in the released papers. As specific cases were not delineated in the presented research, it is not known if some of the cases overlap

between the released studies. It is also unknown if some of the insider threat cases overlap (or are the same as) the cases presented in the previously addressed PERSEREC reports. However, the intent of presenting these summaries, whether or not cases are replicated or overlap, is to obtain an overview of some of the basic motivational characteristics of insider threats.

a. CERT's Computer System Sabotage in Critical Infrastructure Sectors

The most important section of this study in relation to this paper is the section summarizing the majority of the motives for the insiders as part of the key findings. CERT researchers found that a "negative work-related event triggered most [malicious] insiders' actions" (Keeney et al., 2005, p. 14) and that "most [malicious] insider's held a work related grievance prior to the incident" (Keeney et al., 2005, p. 14). Figure 1 shows the breakout of the majority of the motivational factors for insiders in this report.

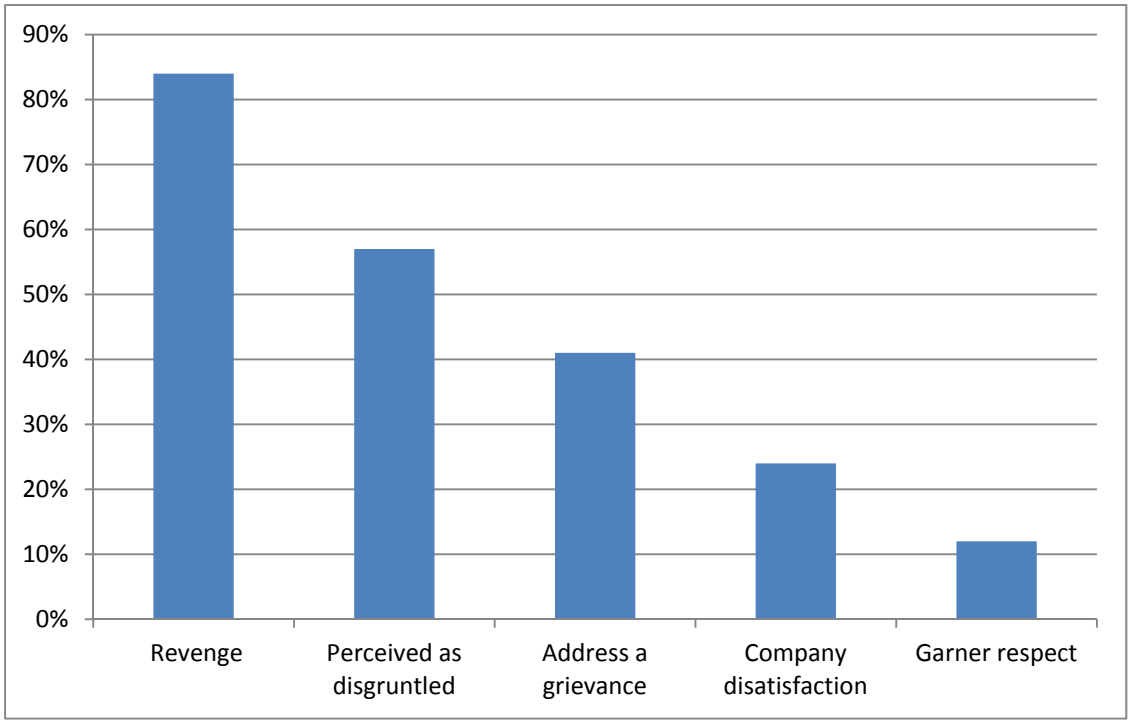


Figure 1. CERT Critical Infrastructure Insider Motivations (After Kenney et al., 2005, p. 41)

b. CERT's Illicit Cyber Activity in the Banking and Finance Sector

Similar to the above study, this research by CERT also produced key findings related to the possible motivations of the insiders. CERT's findings show that most of the insiders were motivated by some sort of financial gain (Randazzo, Keeney, Kowalski, Cappelli, & Moore, 2004). These results, skewed toward a financial motivation, which might be related to the fact that the insiders were working within the financial industry. The motivations from CERT's research are depicted in Figure 2.

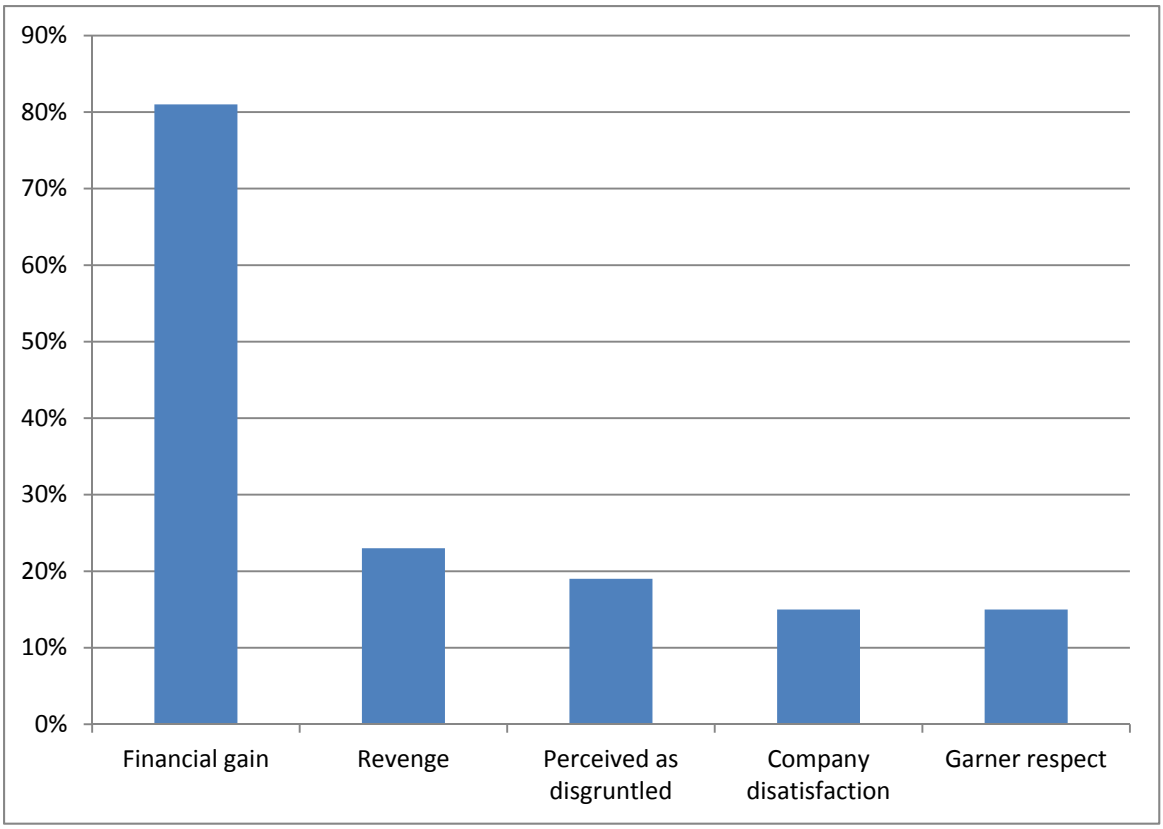


Figure 2. CERT Banking and Finance Insider Motivations
(After Randazzo et al., 2004, p. 12)

c. CERT's Illicit Cyber Activity in the Government Sector

CERT's insider threat study in January of 2008 focused on government employee insider threats. Figure 3 depicts the summary of motivations from this study. Given that the data from this study used in Figure 3 does not address divided loyalties, the questions asked by CERT during their data collection process may not have focused on this motivation for insider threats (Kowalski et al., 2008).

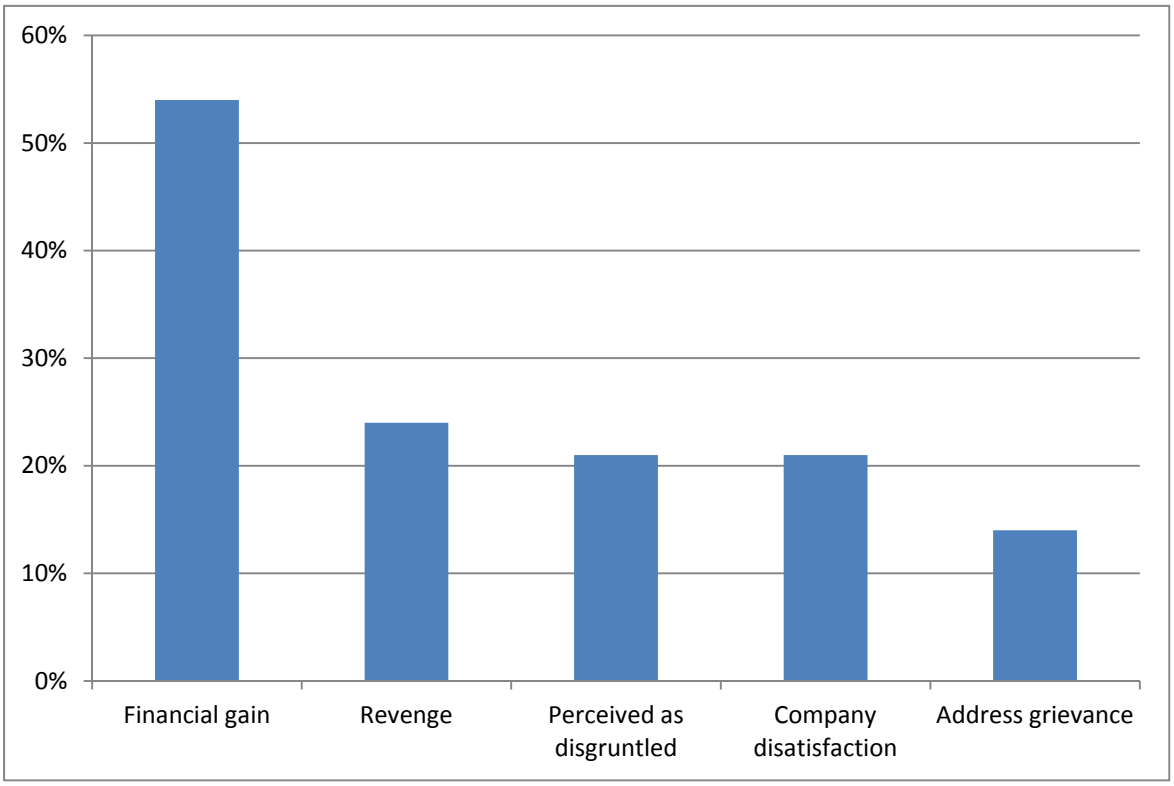


Figure 3. CERT Government Motivations (After Kowalski et al., 2008, p. 16)

d. CERT's Illicit Cyber Activity in the Information Technology and Telecommunications Sector

Also in January of 2008, CERT released their research concerning insider threats inside information technology and telecommunications sectors based on their collected cases (Moore, Kowalski, & Cappelli, 2008). The summaries of their findings concerning the insiders' motivations are depicted in Figure 4.

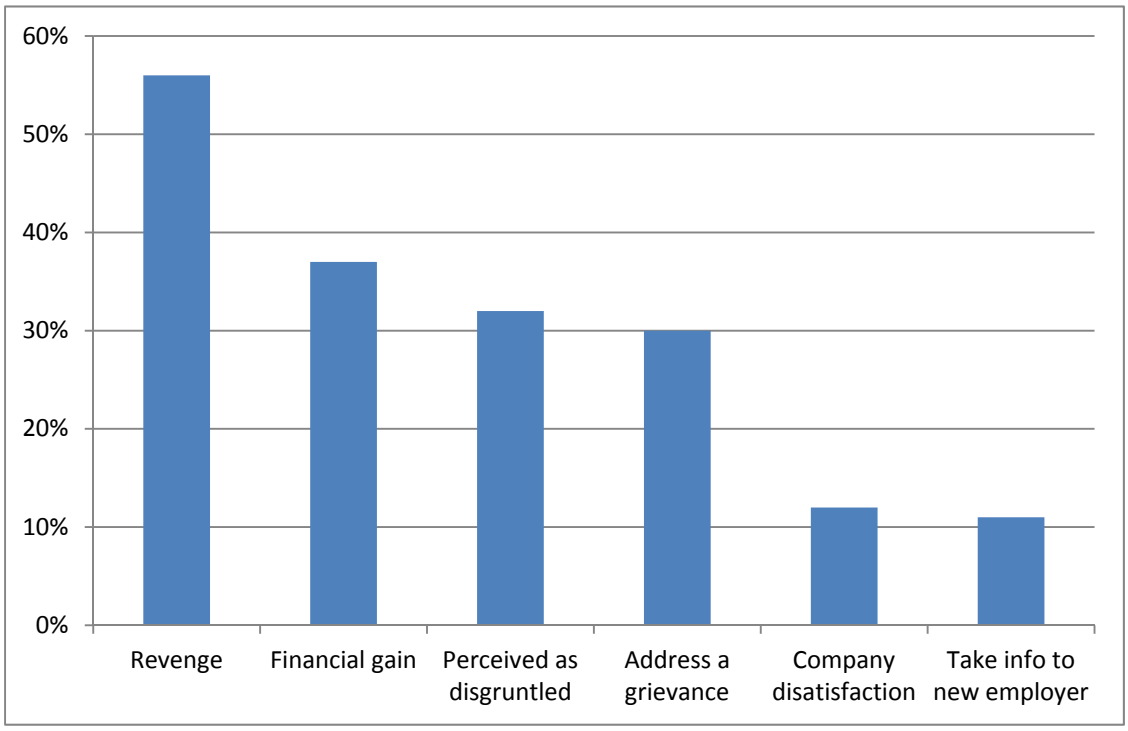


Figure 4. CERT IT and Telecom Characteristics (After Moore et al., 2008, p. 16)

e. CERT Summaries

The previous reports from CERT provide wide-scope coverage of a multitude of historic insider threat cases. In addition to the motivating factors described in the previous sections, these studies also summarized the insiders who had previous arrests prior to the insider incidents and who had come to the attention of either their supervisors or co-workers for some type of adverse workplace behavioral incident. Approximately one third of the insiders for each of the sector summaries had a previous arrest in their background. Also, a significant percentage of the insiders for each sector summary had one or more non-positive workplace incidents that brought their behavior to the attention of their supervisors or co-workers. Figure 5 summarizes these incidents according to the type of CERT report.

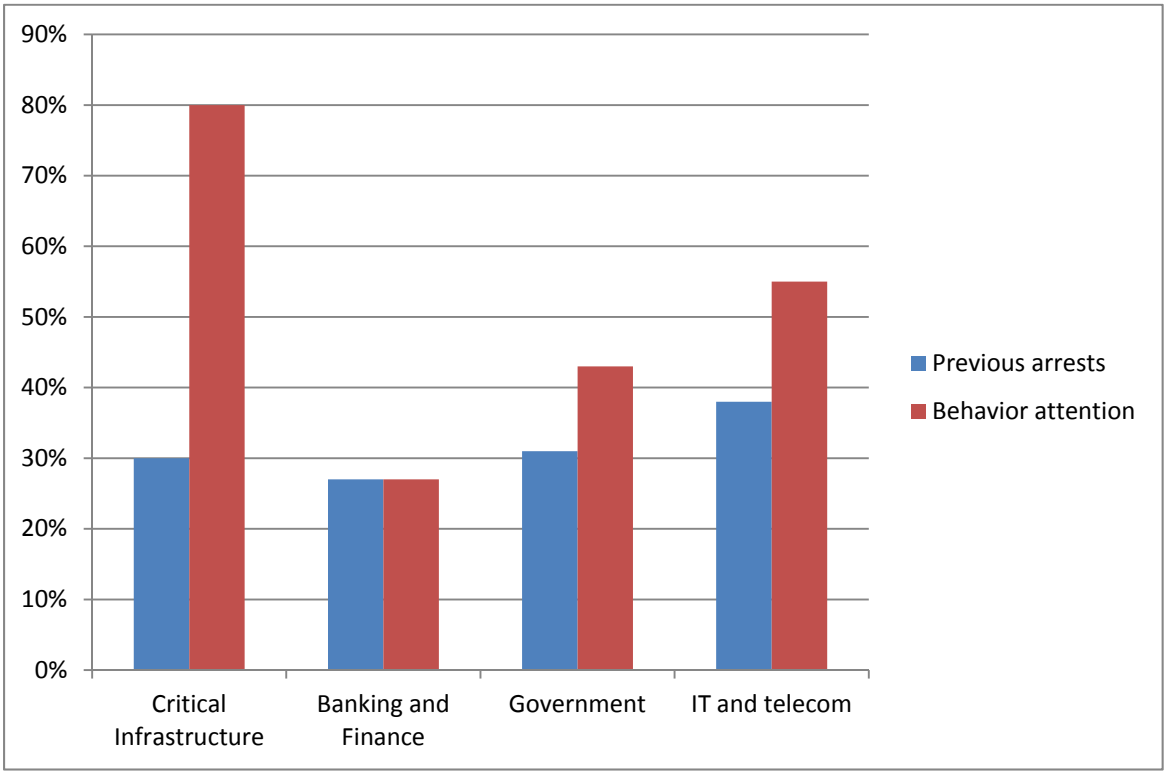


Figure 5. CERT Previous Arrests and Behavior Attention Summaries (After Keeney et al., 2004, Randazzo et al., 2005, Kowalski et al., 2008, and Moore et al., 2008)

D. SUMMARY OF POTENTIAL INDICATORS FOR INSIDER THREATS

As previously discussed, there has been much research conducted on insider threats. The need for insider threat prevention is obvious, but the ability to prevent or even detect insider threats is a difficult endeavor. Employee background indicators can possibly play a role in developing a SIEM rule that would enable automated warnings or detections based upon logical correlations among these indicators.

In the PERSEREC reports, three of the most important factors to consider when attempting to predict insider threat activities are: divided loyalties, finances, and disgruntlement. In the CERT summaries, the most important factors to consider are: employee motivations for financial gain, employee disgruntlement and/or desire for revenge due to a variety of workplace factors. Additionally, employees who have had previous arrests or have come to the attention of their supervisors or co-workers for non-positive workplace behaviors, is also a significant factor for the malicious insider in the CERT reports. While any of these factors alone are not definite predictors of a malicious insider, they can be "weighted" and used as indications and warnings that additional attention and scrutiny are warranted. Most of the motivations summarized above are (or *should* be) addressed in a military person's PSI. Workplace behavioral factors as well as documented administrative actions concerning a given employee's behaviors can both be addressed in the employee's PSI. This will be described in detail in the following chapter.

The data described above can be used as potential events for constructing SIEM rules tailored to users for potential insider threat identification. The following list summarizes the best candidate factors from the PERSEREC and CERT reports to consider in constructing an insider threat SIEM rule:

- Divided loyalties/foreign influence
- Financial difficulties
- Disgruntlement/workplace behavior
- Arrest history

The following chapter will describe the Navy's PSI process as well as typical administrative actions that might facilitate the collection of the above data in order to extract specific items for inclusion in a SIEM rule.

THIS PAGE INTENTIONALLY LEFT BLANK

V. PERSONNEL SECURITY INFORMATION, ADMINISTRATIVE ACTIONS, AND ACCOUNT CREATION

A. DEPARTMENT OF THE NAVY PERSONNEL SECURITY INVESTIGATIONS

In order for a candidate employee to successfully achieve employment at most DoD components, she must voluntarily submit detailed facts about her life. This background information is used to make decisions about an employee's suitability for certain positions. If an employee cannot successfully pass this initial background investigation, they may not be considered for certain DoD positions, or they may not be considered for *any* position within the DON. The DON Clearance Adjudication Facility (DONCAF) is the entity responsible for this process within the DON (Secretary of the Navy, 2006). The following sections will provide a brief overview of this process and highlight how information already collected during a background investigation can be used to tailor a SIEM rule to a user (or groups of users).

1. Types of Personnel Security Investigations

The Navy's Personnel Security manual describes several types of PSIs for personnel depending on their job duties. The basic PSI is the National Agency Check (NAC). This "check" includes fingerprint searches, FBI criminal file searches, and other agencies such as Immigration and Naturalization Services to determine if there is any detrimental information on the specific person being investigated. This is used as the basis for the other, more detailed PSIs (Secretary of the Navy, 2006). The next level up is the National Agency Check with Written Inquiries (NACI). This is the NAC with written requests for information to a person's employers/supervisors, schools, etc. (Secretary of the Navy, 2006).

Another example PSI is the National Agency Check with Local Agency and Credit Checks (NACLC). As the name suggests, this is the NAC with additional credit checks and inquiries to local, not federal, law enforcement entities where the person under investigation has lived. The NACLC is the basis for determining military

suitability for Navy and Marine Corps military personnel, both enlisted and officers. This is considered to be the "standard for determinations of eligibility to access Confidential and Secret classified national security information" (Secretary of the Navy, 2006, p. 6–2). For more sensitive positions, more in-depth PSIs are conducted, such as the Single Scope Background Investigation and other specialized PSIs. However, as the NACLC is more applicable to the majority of Navy and Marine Corps service members, the NACLC will be used as the model for data collection for this research. The NACLC is required for all enlisted members of the Navy and Marine Corps upon their initial entry into military service and is also required for all officers, warrant officers, midshipmen, and ROTC members prior to receiving their appointments (Secretary of the Navy, 2006, p. 6–7). In short, the NACLC is required, at least initially, for all service members in the Navy and Marines.

2. Recurring Requirements

The NACLC is considered to be a valid PSI for a period of ten years. It must be updated every 10 to 15 years (Secretary of the Navy, 2006, p. 6–6) in order for the military personnel to be able to maintain their access to confidential or secret information. (Members requiring higher accesses are required to have investigations every five years.) This is obviously a significant period during which much can change in a person's life. Factors that influence or trigger malicious insider activity can easily arise during this expansive time frame.

In addition to this time frequency, new direction has been provided as to the provision of these PSIs due to the recent federal budget sequester of 2013. Three categories of PSI are no longer authorized until further information is received, at least until after September 30, 2013 (Under Secretary of the Navy, 2013). SSBI-Periodic Reinvestigations (PR), Secret PRs using NACLCs, and requests for expedited investigations, are the three non-mission critical PSI submissions no longer authorized (Under Secretary of the Navy, 2013) unless under specific circumstances or needs as described in this recent memorandum. The temporary cessation of these periodic

"checkups" increases the potential risk of military personnel maintaining access when they might have had that access removed for cause during a normal reinvestigation cycle.

3. Investigation Process

The process a Navy or Marine Corps serviceman or woman goes through in order to comply with the PSI information submission requirements, is to fill out the Standard Form 86, Questionnaire for National Security Positions (U.S. Office of Personnel Management, 2010). This form asks basic questions that will eventually contribute to the determination of the applicant's eligibility for national security positions. The form is submitted to the Office of Personnel Management (OPM) and the background information provided is used to drive the NACLC (or other type of PSI). OPM provides investigative services for all PSIs within DoD (Secretary of the Navy, 2006). OPM conducts their investigations based on the information provided and then forwards the results of their investigations to DONCAF. Upon reviewing the results from OPM, DONCAF determines whether or not a person is eligible for access to the requested level of clearance (Secretary of the Navy, 2006).

4. SF-86 Personnel Security Investigation Questions

As previously described, the SF-86 is the standard form used for most security investigations within the Navy and Marine Corps and requires specific data from users to assist in making an overall clearance and position eligibility decision. The SF-86 requires applicants to submit information on their previous employment, previous residences, foreign influences, financial situations, previous arrests, drug and alcohol use, and many more similar type questions. These questions gather information that is directly related to three of the four insider threat factors identified in the previous chapter. These factors are divided loyalties/foreign influence, financial difficulties, and arrest history. The fourth factor, disgruntlement, might be discoverable through administrative actions which will be discussed later in this chapter. Sections of the SF-86 require reporting any previous firings or administrative action from previous employers (U.S. Office of Personnel Management, 2010). These might indicate a predilection towards employee workplace issues. Personnel may have multiple items on their SF-86 that might trigger further

investigations or cause for concern, but that person can still receive a security clearance if these items are not determined to be serious enough to prevent receipt of a security clearance. Eligibility is determined by common sense and the "whole person" concept (Secretary of the Navy, 2006, p. 7–1). However, this direction to use common sense and evaluate the entirety of the person and her past behavior in determining security eligibility implies subjectivity. Individuals granted eligibility by DONCAF can possibly still become insider threats. SIEM rules using collected personnel data can potentially assist insider threat detection by monitoring a person's network behavior and possibly flagging events of concern.

5. Joint Personnel Adjudication System and the Automated Continuing Evaluation System

The status and eventual results of the investigation can be accessed via the Joint Personnel Adjudication System (JPAS), a web-based application for security managers. This allows local security managers the ability to look up a person's clearance eligibility, status of his current investigation, when the next investigation is due, if non-disclosure forms have been signed, and other related security management items (Secretary of the Navy, 2006). Answers to an applicant's submitted questionnaire can be viewed through JPAS if the local security manager has the appropriate permissions on their JPAS access account (JPAS, 2013). However, if the user already has a completed security clearance on file on JPAS, the specific results of the questionnaire are not as easily accessed.

Once a clearance level has been approved for an applicant, the applicant must apply to both DONCAF and OPM in order to request a copy of the completed investigation, which should include the applicant's responses to the SF-86 questions (Naval Criminal Investigative Service, 2013). Unfortunately, "copies of submitted SF-86's are not maintained electronically in the format in which they were submitted" (Naval Criminal Investigative Service, 2013). Not maintaining these records in an easily accessible format for security managers is one of the barriers that must be overcome in order to effectively use an applicant's responses as potential inputs to a SIEM insider threat rule.

In the future, JPAS will eventually be replaced by a program that will also include continuous evaluation. This system is known as the Defense Information System for Security (DISS) and will include a technology called Automated Records Check. The Automated Records Check in development should provide "more cost effective and timely solutions to obtain commercial and federal records to support investigations" (JPAS, 2013). The Automated Records Check will feed the Automated Continuing Evaluation System (ACES), which will be a part of the DISS family of systems (JPAS, 2013).

ACES will provide a "fully-automated process to query applicant data against appropriate government and commercial databases to collect, analyze, and validate clearance data in order to produce reports that flag potential issues" (JPAS, 2013). The goal is to gain both more fidelity of information, and more frequency of information on personnel who have clearances in order to decrease the threat posed by missing security-related information that might arise during the lengthy periods of clearance reinvestigations. ACES is a tool developed by PERSEREC and first used in a beta test from August 2004 to February 2005, in which it checked over 12,000 individuals holding TS/SCI clearances in between their periodic reinvestigations (Defense Personnel Security Research Center, 2013). As ACES has progressed in its development, it can now audit over 40 databases for items of potential security concern regarding cleared individuals and is currently being used in several pilot programs to evaluate the capabilities of the Automated Records Checks (Defense Personnel Security Research Center, 2013) and will be incorporated into DISS when DISS is projected to replace JPAS in FY2016 (JPAS, 2013).

6. Continuous Evaluation and Reporting Obligations

As there is a significant time gap between clearance reviews and re-investigations, recipients of a security clearance are required to report any changes in their status that might affect their security clearance. The command security officer is designated as responsible for coordinating this continuous evaluation of eligibility for personnel (Secretary of the Navy, 2006, p. 2–4). Some of these mandatory reporting requirements

are changes in marital status, arrests, close and continuing contact with foreign nationals, foreign travel, bankruptcies, etc. (U.S. Office of Personnel Management, 2010).

As previously described, DoD is testing and using the ACES tool to assist in discovering security related items that individuals may fail to report as required. ACES will automatically query government and commercial databases that maintain persons' financial, foreign, and criminal issues (Secretary of the Navy, 2006, p. 10–5). However, if a person with a security clearance fails to self-report these items, either through ignorance or purposeful neglect, or these items are not accessible in a database queried by ACES; these items will not be discovered until that person's next periodic reinvestigation. ACES is not intended to replace the Navy's continuous evaluation and reporting requirements program (Secretary of the Navy, 2006, p. 10–5).

PERSEREC describes one of the possible future uses of ACES to trigger "expanded investigations when it detects new issues" (Defense Personnel Security Research Center, 2013). This could potentially be used as input for a SIEM rule to specifically look for an individual's network activity related to the ACES discovery. This would be similar to using an individual's SF-86 information as inputs to SIEM rules. How ACES will actually be utilized with the enhanced Automated Records Check within the new DISS will determine how information discovered during its queries can be used for SIEM rules or watch lists. Information collected during the PSI process, and possibly during ACES queries, can be used for rules tailored to a specific user. This can potentially augment the continuous evaluation process required by the Navy.

B. NAVY ADMINISTRATIVE ACTIONS

With any organization, there are numerous administrative actions required in response to an employee's actions or offenses. These administrative actions could potentially be used to identify employees who might be at risk of evolving into insider threats. There are a variety of options available to a commander. They include counseling and nonpunitive censure, nonjudicial punishment, and courts-martial (Judge Advocate General, 2012).

There are many specific options available to a commander under each of the main categories and each option may result in documentation potentially useful for SIEM inclusion. In the following section, counseling and nonjudicial punishment will be examined in order to highlight how information resulting from these actions could be incorporated as input to a SIEM for preventing or discovering insider threats related to potential disgruntlement.

1. Counseling

Counseling is "intended to give a member the opportunity to improve by identifying specific, undesirable behavior, which the member must alter or cease" (Deputy Chief of Naval Personnel, 2009, p. 1910–202). Counseling is a broad category that can be conducted verbally or in a written format. Verbal counseling is not documented and is not useful for consideration as a possible data point for inclusion into a SIEM for the purposes of this research. Formal counseling can be documented in an individual's service record utilizing NAVPERS form 1070/613 Administrative Remarks, commonly referred to as a Page 13 entry. This entry is used to document a variety of items, both positive and negative, for a service member.

One example of counseling that could result in a Page 13 entry into an individual's service record is an individual's failure to pass the Navy's required physical fitness assessments. If a service member fails to meet the minimum standards three times within a four-year period, then the service member will be processed for administrative separation from the Navy (Chief of Naval Operations, 2011). If an individual has multiple failures and is close to being considered for administrative separation, this might be an item to include on a SIEM watch list or rule for that individual. An individual close to being administratively separated might become disgruntled, one of the possible indications of insider threat as discussed in previous chapters.

While there may be nothing else to indicate the person is disgruntled, being separated from employment is a traumatic event and should invite further scrutiny of that person's activities as a preventive measure in case of actual disgruntlement. A precautionary measure would be to use this information as part of that person's overall

profile utilized by a SIEM in order for the SIEM to monitor for potentially suspicious activity by that person. Documenting physical fitness failures is just one of numerous administrative remarks in a service member's record that can potentially be used as part of a SIEM.

2. Nonjudicial Punishment

Nonjudicial punishment (NJP)—also known as Captain's Mast, Article 15, or Office hours depending on the service branch—can be used, depending on the circumstances, instead of courts-martial (Judge Advocate General, 2012). This is not a criminal trial but it is a disciplinary proceeding designed for minor misconduct (Judge Advocate General, 2012). There are many personal actions/infractions that can result in nonjudicial punishment. Despite the offense or punishment received, there will be a service record entry using the NAVPERS form 1070/613 Administrative Remarks (Judge Advocate General, 2012). Since NJP can adversely impact an individual's career, it is another potential SIEM cueing item that could be correlated to indicate possible disgruntlement.

The preceding items recorded in an individual's service record are just a few of many possible administrative actions that could be incorporated into a SIEM to monitor for potential insider threat activity. However, some of these items might not be considered for an individual's clearance or allowed accesses until the individual's reinvestigation; unless specified by the commander, or if the nonjudicial punishment was directly related to a security incident or violation.

These administrative actions can be taken into consideration for the overall security clearance determination as they might serve as motivators for potential disgruntlement. However, the significant time gap between investigations leaves a period within which a potentially disgruntled employee might develop into a malicious insider with no SIEM-observable warning indicators. Including these administrative items for SIEM monitoring might assist in discovering these threats during the long intervals between security clearance investigations. The current method by which individuals can receive a network account within Navy commands should also be examined in order to

determine possible ways a command might be able to use the previously described information from both the SF-86 and administrative actions.

C. SYSTEM ACCOUNT ACCESS REQUEST

When an individual first check's into a Navy command, there is typically a standard check-in process. The individual will receive a command check-in sheet, which she must take to the command's various departmental representatives. These departmental representatives will provide the new check-in with necessary information concerning the command and then sign the individual's check-in sheet. One of the key items for a newcomer is to receive necessary system accesses in order to conduct the duties of their position. This person may require multiple accounts and accesses with varying classifications depending on their responsibilities. In order for the new check-in to receive network access or accounts, she will fill typically out the System Authorization Access Request-Navy (SAAR-N) OPNAV 5239/14 form. This form collects a variety of information on the new check-in in order to provide system access. There are four parts to this form.

1. SAAR-N Part I

Part I gathers basic information such as the employee's name, department, job title, phone number, etc. It also includes checkboxes for the employee's citizenship and whether she is military, civilian, or contractor, and whether information assurance training has been completed. Part I of the SAAR-N is shown in Figure 6:

E-MAIL SUBMIT

FOR OFFICIAL USE ONLY WHEN FILLED

SYSTEM AUTHORIZATION ACCESS REQUEST NAVY (SAAR-N)

PRIVACY ACT STATEMENT

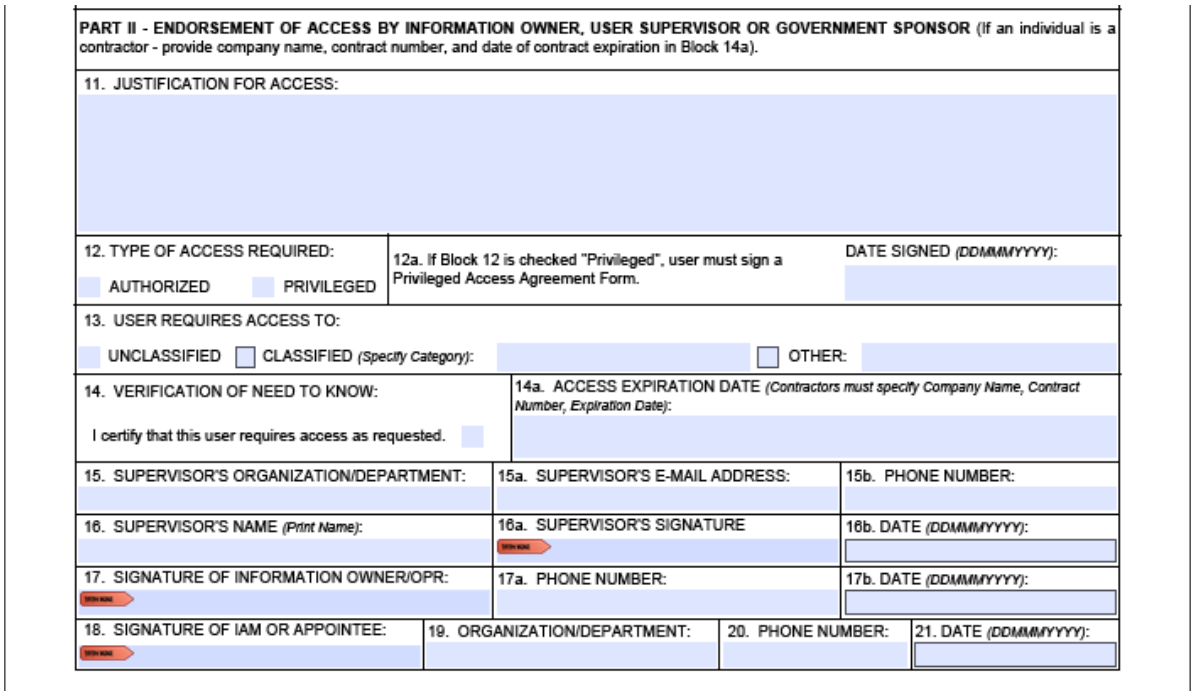
AUTHORITY: Executive Order 10450, Public Law 99-474, the Computer Fraud and Abuse Act; and System of Records Notice: NM0500-2 Program Management and Locator System.
PRINCIPAL PURPOSE: To record user identification for the purpose of verifying the identities of individuals requesting access to Department of Defense (DOD) systems and information.
ROUNTINE USES: The collection of data is used by Navy Personnel Supervisors/Managers, Administration Office, Security Managers, Information Assurance Managers, and System Administration with a need to know.
DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

TYPE OF REQUEST: ☐ INITIAL ☐ MODIFICATION ☐ DEACTIVATE ☐ USER ID	DATE *(DDMMMYYYY)*:
SYSTEM NAME *(Platform or Application)*:	LOCATION *(Physical Location of System)*:
PART I ***(To be completed by Requester)***	
1. NAME *(Last, First, Middle Initial)*:	2. ORGANIZATION:
3. OFFICE SYMBOL/DEPARTMENT:	4. PHONE *(DSN and Commercial)*: DSN: COM:
5. OFFICIAL E-MAIL ADDRESS:	6. JOB TITLE AND GRADE/RANK:
7. OFFICIAL MAILING ADDRESS:	8. CITIZENSHIP: ☐ US ☐ FN ☐ LN ☐ Other
	9. DESIGNATION OF PERSON ☐ MILITARY ☐ CIVILIAN ☐ CONTRACTOR
10. INFORMATION ASSURANCE (IA) AWARENESS TRAINING REQUIREMENTS *(Complete as required for user or functional level access.)*:	
☐ I have completed Annual IA Awareness Training.	DATE *(DDMMMYYYY)*:

Figure 6. From SAAR-N (OPNAV 5239/14, 2011) Part I

2. SAAR-N Part II

The first section of Part II includes a section for justification of access, type of access required, classification of access required, supervisor's information and supervisor's verification of the employee's need to know. The remainder of Part II includes a detailed user consent agreement which the user signs. The user's signature indicates they will adhere to the policies and also consent to monitoring. The first section of Part II of the SAAR-N form is shown in Figure 7:



PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR (If an individual is a contractor - provide company name, contract number, and date of contract expiration in Block 14a).

11. JUSTIFICATION FOR ACCESS:

12. TYPE OF ACCESS REQUIRED: AUTHORIZED PRIVILEGED

12a. If Block 12 is checked "Privileged", user must sign a Privileged Access Agreement Form.

DATE SIGNED *(DDMMMYYYY)*:

13. USER REQUIRES ACCESS TO: UNCLASSIFIED CLASSIFIED *(Specify Category)*: OTHER:

14. VERIFICATION OF NEED TO KNOW: I certify that this user requires access as requested.

14a. ACCESS EXPIRATION DATE *(Contractors must specify Company Name, Contract Number, Expiration Date)*:

15. SUPERVISOR'S ORGANIZATION/DEPARTMENT:

15a. SUPERVISOR'S E-MAIL ADDRESS:

15b. PHONE NUMBER:

16. SUPERVISOR'S NAME *(Print Name)*:

16a. SUPERVISOR'S SIGNATURE

16b. DATE *(DDMMMYYYY)*:

17. SIGNATURE OF INFORMATION OWNER/OPR:

17a. PHONE NUMBER:

17b. DATE *(DDMMMYYYY)*:

18. SIGNATURE OF IAM OR APPOINTEE:

19. ORGANIZATION/DEPARTMENT:

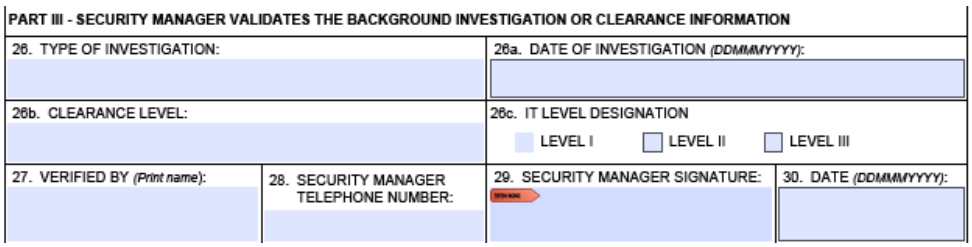
20. PHONE NUMBER:

21. DATE *(DDMMMYYYY)*:

Figure 7. From SAAR-N (OPNAV 5239/14, 2011) Part II

3. SAAR-N Part III

Part III is for use by the security manager and requires a signature indicating the type of background investigation and clearance information concerning the applicant. The security manager will enter the type of investigation (NACLC, SSBI, etc.), the date of investigation, the clearance level the individual has, and the IT level designation of that individual. The IT level is used to determine special privileges the applicant might require depending on their required duties. Level I indicates privileged access, Level II indicates limited privilege with sensitive information access, and Level III indicates no privilege and no sensitive information access (Secretary of the Navy, 2006). Part III is shown in Figure 8.



PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION

26. TYPE OF INVESTIGATION:

26a. DATE OF INVESTIGATION *(DDMMMYYYY)*:

26b. CLEARANCE LEVEL:

26c. IT LEVEL DESIGNATION LEVEL I LEVEL II LEVEL III

27. VERIFIED BY *(Print name)*:

28. SECURITY MANAGER TELEPHONE NUMBER:

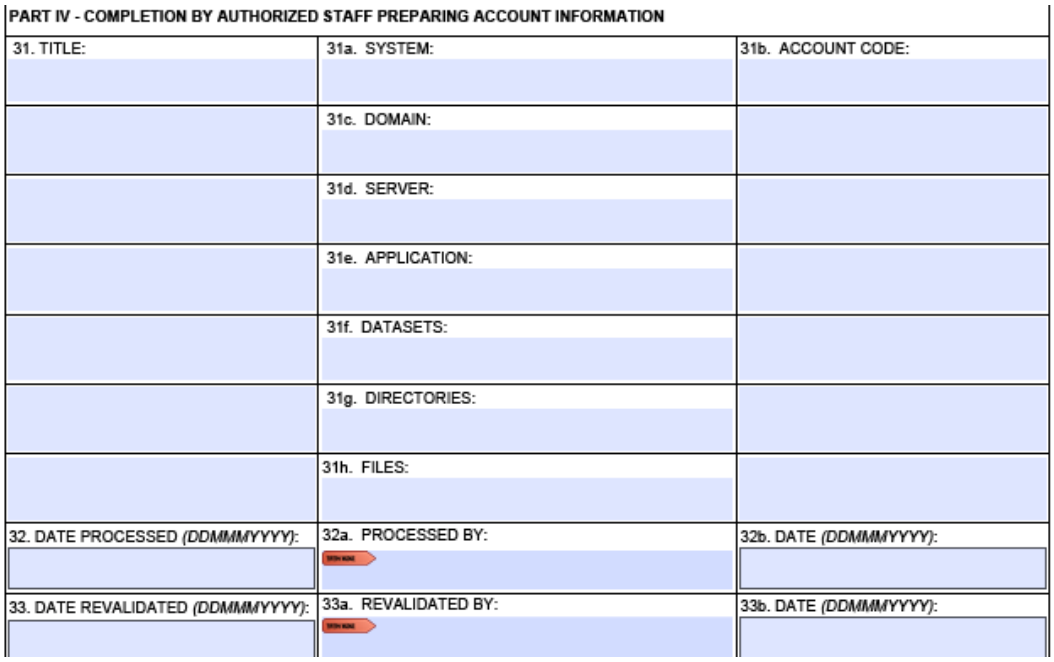
29. SECURITY MANAGER SIGNATURE:

30. DATE *(DDMMMYYYY)*:

Figure 8. From SAAR-N (OPNAV 5239/14, 2011) Part III

4. SAAR-N Part IV

Part IV is used to identify the specific accesses an individual may require as part of their job duties. SAAR-N Part IV is shown in Figure 9.



PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION		
31. TITLE:	31a. SYSTEM:	31b. ACCOUNT CODE:
	31c. DOMAIN:	
	31d. SERVER:	
	31e. APPLICATION:	
	31f. DATASETS:	
	31g. DIRECTORIES:	
	31h. FILES:	
32. DATE PROCESSED *(DDMMMYYYY)*:	32a. PROCESSED BY:	32b. DATE *(DDMMMYYYY)*:
33. DATE REVALIDATED *(DDMMMYYYY)*:	33a. REVALIDATED BY:	33b. DATE *(DDMMMYYYY)*:

Figure 9. From SAAR-N (OPNAV 5239/14, 2011) Part IV

5. SAAR-N Summary

Parts III and IV of the SAAR-N are potentially areas where more detailed information about the user might be included for use by a SIEM. For example, in Part III, instead of only listing the investigation completed and the clearance level, there might be a section to include some of the individual's responses to SF-86 questions that might be considered as having an extra risk for that individual becoming an insider threat. It could also be a place to list administrative actions received by that individual. These questions and administrative actions could be related to the potential precursors of insider threats previously examined in Chapter III, foreign influence/divided loyalties, financial difficulties, disgruntlement, and previous arrests.

While the investigative process determined the eligibility for the individual to receive a clearance to obtain certain accesses, this would be a way extract more detailed information about the individual in order to incorporate that person's data into a SIEM watch list or rule. For example, if a person has SF-86 responses indicating previous financial difficulties, that could be listed on the SAAR-N in some format and the system administrator or commander would be able to use that information to add that person's name or user account to a SIEM watch list. This watch list would then be used with SIEM rules to monitor that person's network activities for a variety of activities that might indicate potential insider threat type activities.

D. SUMMARY

Data is gathered and recorded during military Personnel Security Investigations and administrative actions that can potentially provide details useful for a SIEM to monitor for malicious insider activities. While the specific data from an individual's SF-86 is currently difficult to access, it might be possible to include specific responses to SF-86 questions related to potential insider threat indicators as part of that person's JPAS entry for use by the local command security manager. This would allow for the data to be in a centralized location accessible by each command security officer responsible for that individual. Additionally, administrative actions recorded in an individual's service record can provide information useful for SIEM monitoring, especially in cases of potential employee disgruntlement.

The process might work in the following manner: When an employee checks into a command, a modified type of the SAAR-N could include areas for the command security officer to list potential insider threat flags produced by the SF-86 questions and documented in the individual's JPAS file. Administrative personnel might list documented administrative actions from the individual's service record. These items could then be used by personnel responsible for approving the SAAR-N to develop a user profile based on this information. This profile could be used for watch lists and rules with a SIEM to enhance a command's ability to prevent and discover malicious insiders.

In order for this process to function, there would need to be SIEM rules developed that would specify what types of activity should be monitored. It is unlikely that any combination of rules, however well chosen and logically combined, will be able to capture all the ways in which an insider could possibly cause damage. However, by identifying individuals with backgrounds containing potential indicators as previously described, and applying SIEM rules to those individuals, alerts can be designed to inform designated personnel of an individual's network activities that may indicate potential malicious activities. These network activities may not be singularly indicative of a malicious insider, but, when taken in conjunction with background factors, they may require further investigation to prevent or discover malicious insider activity.

One malicious insider activity, specifically within the U.S. military, is the release of information, classified or unclassified, outside of the military's control without proper authorization. Sample data extraction methods by malicious insiders will be examined in the following chapter. These methods can be incorporated into a SIEM rule or rules for monitoring previously identified users.

VI. SELECTION OF CANDIDATE EVENTS FOR SIEM CUEING

A. DATA EXFILTRATION METHODS AND LOG EVENT SOURCES FOR SIEM CORRELATION

Understanding the variety of ways in which an insider can cause damage to any organization is an important component of combatting the insider threat. One potentially devastating way an insider can threaten or attack an organization is to steal information. For the military and U.S. government, this information can range from classified to unclassified data. However, regardless of the classification of the data, every portion of data stolen or otherwise obtained by an insider provides potential advantage to an adversary. This data compromise can lead to economic damage, political damage, and even deaths of military or other government operators.

Recognizing the ways in which data can leave an organization without authorization, can assist in developing SIEM rules to generate alerts or warnings if some of these data extraction activities are observed. The following will briefly describe some of the ways that an insider can remove data from an organization.

1. Printing

An historic example of printers being used in insider espionage is the case of Robert Chaegun Kim, a computer specialist working for the DON at the Office of Naval Intelligence. Kim was formerly a citizen of South Korea, prior to becoming a U.S. citizen. Kim used his insider access at ONI to find classified documents, delete the classification markings, and then print them out to mail to his South Korean contacts (Defense Personnel Security Research Center, 2009). Another example is the case of Leandro Aragoncillo, a naturalized U.S. citizen from the Philippines. Aragoncillo used his insider access while working at the FBI as an intelligence analyst to pass classified information to the Philippine government. He would search the FBI files, then download and print out documents concerning the Philippines (Defense Personnel Security Research Center, 2009).

Most organizations, whether commercial, government, or military, allow insider usage of printing facilities. This is an obvious necessity in order for the users to conduct their day-to-day activities in fulfillment of their employment requirements. There are two common ways in which an organization can configure its printing services for its users. A printer can be directly connected to a user's workstation for their sole use or a printer can be configured on a network for many users to share.

For cost saving purposes, it is generally most efficient to have a shared printer. Depending on the size of the organization, the segregation of shared printers might be conducted by work function, location, or other factors. A user with a dedicated printer might have specialty functions that require sole usage of the printer or the user might be in some sort of elevated position within the organization where they need their own printer and cannot afford to share the printing service with others.

Most modern printers contain logging capabilities that record activities such as user, time accessed, pages printed, file names, and other data fields depending on the printer manufacturer or on the fields set by the installer or network administrator. Connecting a shared printer to a SIEM to collect, aggregate, and normalize these logs would allow for continuous monitoring of user's printing activities. Connecting dedicated printers would also provide this function, but it might be more cost-effective for an organization to begin with shared printers as this facilitates printer monitoring for a greater number of users. However, there is still a risk that individuals with dedicated printers might find it easier to conduct illicit printing activities, without the fear of observation, if the printer is not networked with other users. Certain aspects of the shared printing services can be input into the SIEM rule for correlation or alerts (Holloway & Santiago, 2012) depending on the organization, but it is important to have a general idea of what the baseline, or normal, printer usage is prior to implementing these SIEM rules in order to reduce false positives.

a. Time of Use

Time of use of the printing service can be significant in detecting potential insider threats (Holloway & Santiago, 2012). If a user is printing after hours, it might be

that the user is attempting to avoid co-workers or supervisors from directly observing what he is printing. This insider could be: just working after hours on official tasks, simply abusing the printer for personal use, or potentially printing out sensitive data for extraction or exploitation.

b. Quantity of Use

Large amounts of print jobs for a particular insider might be another metric to cue a SIEM alert on (Holloway & Santiago, 2012). A sudden increase in the volume of pages or of files sent to a printer by a particular user might be one factor that, once correlated with other information, might indicate a potential insider.

c. Types of Files

The types of files sent to a printer by a user can indicate potential insider threats in several ways. If a user is sending files to the printer that are outside the normal scope of that user's job responsibilities, that could be viewed as an indicator (Holloway & Santiago, 2012). If a user prints out databases, slides, word documents or excel documents, depending on their job responsibilities, those could also be indicators. This level of detail for printer usage would probably best be used as a correlating factor for a SIEM rule. For example, if a user's background data shows connections to a foreign country, and then that user is found to be printing files related to that foreign country; this is likely worthy of added investigative attention.

2. Copiers

An organization's copy machine can also be used in a similar manner to a printer for potential identification of malicious activities. A copy machine is capable of recording and generating logs with similar fields as a printer; which can also be delivered to a SIEM for further analysis. Unfortunately, many copy machines currently in use do not employ identity-based access controls that would be able to provide a user identity in conjunction with any given copy job. Additionally, some copy machines are not network capable, which precludes the forwarding of log data to a SIEM. For example, David Sheldon Boon, an Army signals analyst for NSA, used a handheld scanner to copy

classified documents that he later passed to the Soviets (Defense Personnel Security Research Center, 2009).

a. Time of Use

Like the printer, the time when a copy machine is used might be a cue for further investigation, or at least as an input for correlation against other tripwires or indicators. Baselines should also be understood in order to reduce false positives.

b. Quantity of Use

Large increases in copy machine usage in volume of pages or files could be used to indicate insider threat activity as previously discussed in regards to printer usage.

c. Types of Files

Depending on the type of copy machine in use by an organization, the types of files copied may or may not be available or supported. The log fields for a copy machine may not differentiate between documents, spreadsheets, slide shows, or images reproduced.

3. E-mails

Most commercial, government, and military users incorporate e-mail activities as crucial components of their day-to-day employment activities. Quick communication is necessary for the smooth flow of an organization's established processes. However, like most other services, e-mail capabilities can be exploited by malicious users (Capelli et al., 2012). One historic example of using e-mails for malicious activity is the case of John Reece Roth, a University of Tennessee professor of plasma physics. He was charged with relaying sensitive information to China, and in one instance had sensitive files e-mailed to him while in China (Defense Personnel Security Research Center, 2009).

Depending on an organization's e-mail policies, there are ways in which a user's e-mail usage can provide indicators as to potential or actual insider threat activities.

a. E-mail Destinations

Depending on the job function of a government or military employee, they will typically send e-mails with the .gov or .mil domains during the normal course of their business. Employees dealing with contracts, research, education, or a variety of other activities will obviously interact with more domains than these two; so, again, the importance of establishing a baseline for normal behavior is emphasized in order to reduce false-positives. Just sending e-mails to other domains is by no means any sort of indicator of maliciousness; but if correlated with other activities, it might be something a SIEM rule should generate an alert for (Holloway & Santiago, 2012).

b. E-mail Attachments

Employees typically send attachments to others via e-mail as a normal part of their workday. However, if an employee is sending attachments to web-based e-mail services or to any potentially suspicious recipients, this might be indicative of data or information leaving the organization without proper oversight (Capelli et al., 2012). Also, there may be network policies or restrictions in place that restrict the size of outgoing attachments. If this is the case, the frequency of the e-mails might be an indicator of malicious activity if an employee is attempting to split up a file in order to exfiltrate the entire amount without tripping network policy size restrictions.

c. Frequency of E-mail

Massive amounts of e-mail to specific locations might be a tripwire for further investigation by security personnel (Holloway & Santiago, 2012). There could be official reasons for this activity; but there could also be the possibility of the employee abusing the organization's network for either personal use or for malicious activity. If the employee also has previous flags on their user profile in regards to their PSI or administrative action, this should warrant further investigation. This further investigation can be programmed into the SIEM for issuing alerts and e-mail notices to appropriate personnel for action.

d. Time of E-mail

Depending on an employee's position and job requirements, the time of e-mails might be indicative of malicious events (Holloway & Santiago, 2012). This is another example of a potential indicator that requires a refined baseline in order to prevent false positives For example, if the e-mail server logs show an employee is sending e-mails after hours; it could indicate several possibilities. The employee might simply be working late on their job requirements, the employee might be using company e-mail for personal purposes, or the employee might be trying to exfiltrate data without supervisors or co-workers looking over their shoulders during the day and observing their activities. These are just a few of the numerous reasons an employee might be sending innocuous e-mails after hours. But, if this activity adds to a set of indicators, the aggregate should trigger further investigation.

4. Web Posts

Web postings by employees in this case means any time an employee is posting information to public websites. This could mean commenting on news articles on websites such as CNN, commenting on opinion blogs, posting pictures or other files to public sites, etc. This could also mean transferring information to a password-protected website (Capelli et al., 2012). Monitoring this activity would most likely be difficult using a SIEM, especially if a user is conducting most of their posting activities to a social network site such as Facebook. However, a SIEM rule could be made that will alert on excessive usage of some of the well-known sites, which might cause a supervisor to conduct further analysis of their employees' on-line activities. In addition to monitoring the frequency of these sites, the SIEM could be used to monitor on file sizes leaving the organization's network.

5. Cloud Services

With the massive increase in data storage capacity offerings by commercial providers, the ability to access data in the "cloud" has greatly increased as well. Many services, such as Amazon Simple Storage Service (S3), offer free accounts with up to

5 GB of free storage (Amazon Web Services, 2013). Regardless of the type of cloud service used, there can be potential for abuse as an exfiltration tool for malicious insiders.

Blocking these cloud services to users might be the simplest solution, but there might be some instances where employees need to use some of these public cloud services as part of their job requirements. In either case, SIEM rule elements could include domain names associated with cloud providers/services for select users whose previous behavior, as documented on their PSI or administrative actions, indicates they are deserving of added scrutiny.

6. Chat Services

Chat services are another way a malicious insider might use to leak data outside of the normal oversight channels. However, this might be extremely difficult to detect with a SIEM as the postings inside chat sessions are generally short and short-lived. But, if an employee is using chat and that is not required as part of their job duties, this could also be used to trip a SIEM rule for further investigation.

B. SUMMARY OF CANDIDATE EVENTS FOR SIEM CUEING

The data exfiltration methods and related log sources described above are just a few of the many possible ways data might leave an organization without appropriate authorizations. Incorporating these methods into a SIEM rule can potentially assist an organization in cueing for malicious insider threat activities. Applying these rules to user accounts that have previously defined flags related to previous PSI information and administrative actions can assist in increasing the fidelity of the system monitoring as described in some of the previous examples. Specific SIEM watch list and rule examples related to potential insider threat indicators and data exfiltration methods will be examined in the following chapter in order to highlight the actual watch list and rule creation process.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. SIEM ARCHITECTURE

A. DETER, PREVENT, DETECT, AND CORRECT

The implementation of a SIEM at a Navy command should address four basic goals as the end state of the SIEM working process as applied to the insider threat. These goals are to *deter*, *prevent*, *detect* and *correct*.

1. Deter

The first goal is to deter the insider threat via fear of discovery and punishment. Command security policies and training can all assist in reaching this goal. Some degree of deterrence would be expected owing solely to the knowledge of the existence of a SIEM capability within the command's network architecture. So if, during the command check-in process, an individual is made aware that their background data is being used in conjunction with their network activities, this might be deterrence enough for some individuals. Knowing that their specific background data is included in a monitoring process might influence some individuals enough to not conduct any suspicious network activities that might draw management attention. Others, however, may be sufficiently motivated to risk detection and punishment and thus *preventive* measures would be the next line of defense.

2. Prevent

Prevention in this context refers to either a) the ability of a SIEM to potentially identify indications of an individual leaning towards becoming an insider threat, or b) early detection of insider actions that are preliminary *to* an actual damaging attack, but which are detected and countered prior to suffering any such damage. An example of this later issue (b) would be data intended for exfiltration, which is moved from a more secure server (perhaps inaccessible from the Internet) to a server directly accessible from the Internet. Design of a SIEM architecture that can monitor and record predefined activities that may indicate potential insider activities can assist the command in preventing the threat from becoming an actuality. By including mechanisms to record individual activity

that may be suspicious, especially when correlated with the individual's previous behavior, the command can further focus on those individuals if necessary. Intervention and further investigation by the command at certain points within the architecture can then potentially prevent the insider from actually conducting malicious activities. However, if the command is unable to prevent malicious insider activity, the SIEM should be able to assist the command in *detecting* actual malicious insider activities.

3. Detect

A SIEM can be designed to notify management or certain individuals such as the security officer or commanding officer if certain pre-defined events occur and are captured by the SIEM. For example, if a SIEM rule is implemented that informs management of a large e-mail sent after-hours, then the SIEM can send an alert e-mail to management and/or add pertinent information regarding this event to a "watch" list maintained by the SIEM. This alerts the management of an activity that may warrant further investigation, and the command can then proceed to identify what information left the command and why it occurred after-hours. This "cue" of a potentially malicious event focuses the command on detecting the specifics of the activity and then facilitates *corrective* action.

4. Correct

Using the cues from the SIEM, the command's management can take corrective steps to reduce the adverse impact resulting from the insider attack. This may require the command to issue a message regarding the potential compromise of sensitive information, notify the Naval Criminal Investigative Service regarding the issue, discipline the individual involved, or other actions as appropriate for the situation and environment.

B. ARCSIGHT EXPRESS COMPONENTS

As described in the previous chapters, an individual's background data gathered from their PSI and administrative actions may help *focus* a SIEM on that person's network activities, with the goal of identifying any possible inclinations towards

malicious activities. Within the ArcSight Express package, active lists, filters, and rules can be designed in a way to provide this capability. Active lists and filters specific to ArcSight Express are briefly described in the following sections.

1. Active Lists

Active lists are comparable to a type of watch list as described in previous chapters. Active lists are typically used within ArcSight Express in "conjunction with rules specifically tailored to interact with and populate the lists dynamically" (ArcSight, 2011, p. 518). Rules are written to populate the list with certain data items of interest. Basically, the active list is a "shell to store/display the data" (ArcSight, 2011, p. 518) populated by any particular rule. In addition to being populated *dynamically* with rules-driven data, active lists can also be populated *manually* with static entries (ArcSight, 2012, p. 64). Active lists can also be used as input conditions for use in other rules.

2. Filters

Filters can be used as building blocks for rules and "are a set of conditions that focus on a particular set of event attributes" (ArcSight, 2012, p. 57). Filters serve to limit the number of events processed by the system, focusing only on the desired events (ArcSight, 2012, p. 57). They can also be used to specify conditions within rules. For example, filters can be created and applied to log sources, such as a printer. The filter can specify that only events exceeding certain limits, such as print batch sizes, or certain operational hours, such as after hours; are used by the specified rule for processing (Holloway & Santiago, 2012). Multiple filters from multiple log sources can be applied as condition statements feeding into a single rule.

C. SAMPLE SIEM ARCHITECTURE WITH FILTERS, ACTIVE LISTS, AND BOOLEAN RULES

Within ArcSight Express, there are many potential ways to organize the components in order to achieve the previously defined goals as related to the insider threat. One possible organization of ArcSight Express's capabilities utilizes the basic components of active lists, filters, and rules in order to monitor for potential malicious

activities. This architecture focuses on using multiple active lists grouped by specified PSI, administrative events, and individual clearance levels; combined with multiple active lists grouped by specified network activities. This example is one of many potential ways to design the architecture based on specific Navy command size, mission, network components, etc.

For this paper, the proposed example architecture uses multiple, grouped active lists. The architecture in this section can be used as a starting point for utilizing a SIEM tool to address insider threats. This design includes both manual inputs and automated inputs. Figure 10 provides an overview of this design.

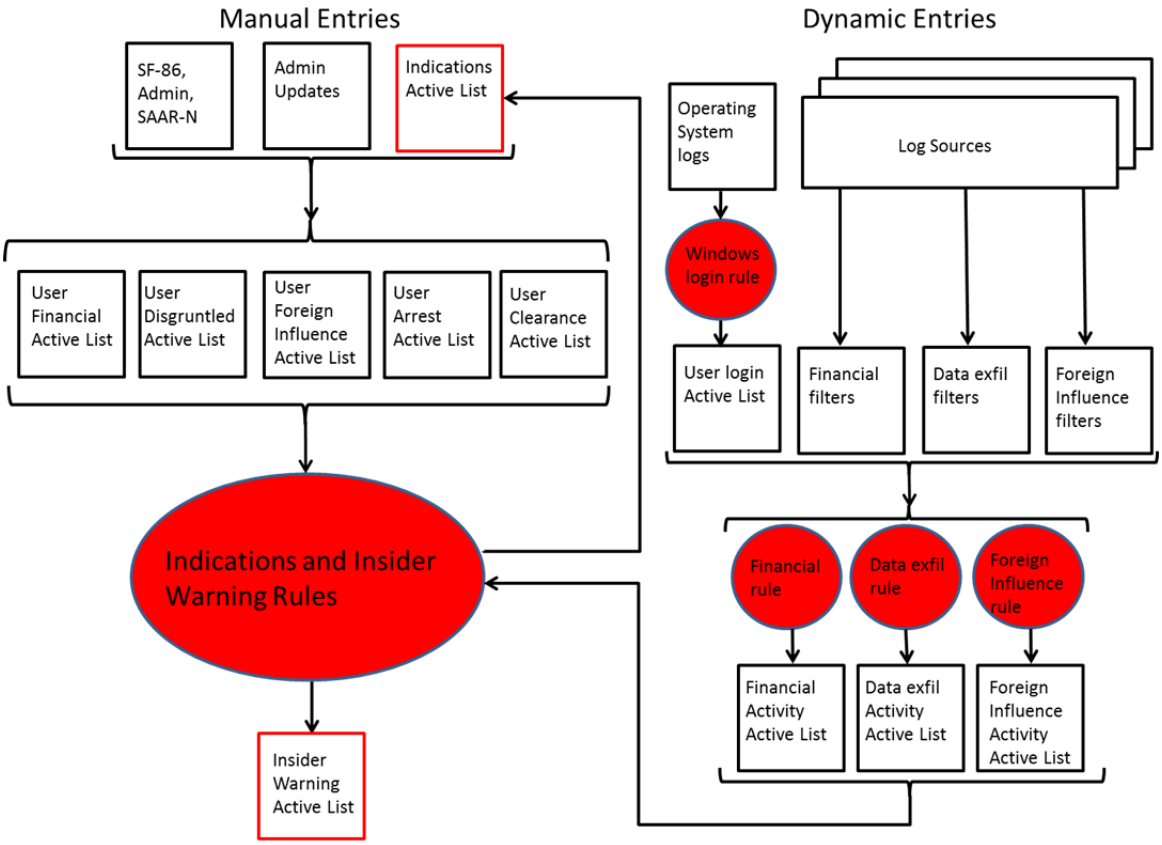


Figure 10. Architecture for SIEM implementation

The process begins when a new user checks into a command. This user will have the security officer and administrative officer check their JPAS account for any security flags based on answers to SF-86 questions (if JPAS or its replacement eventually allows for these specific details to be represented). If there are any security flags, the security officer documents them on the individual's SAAR-N form. Additionally, the security officer will document the clearance level of the new user. The same process is repeated by the administrative officer. If there are any items of interest, such as physical fitness test failures, nonjudicial punishment, etc., these are documented on the SAAR-N form.

When the system administrator (or responsible entity) receives the SAAR-N form from the individual, she then makes an account for the new user with whatever accesses are typically required. The system administrator manually enters any information from the SAAR-N related to the potential indicators of malicious insider activities as described in Chapter III (foreign influence, financial issues, disgruntlement, previous arrests) as well as the clearance (if any) of the individual into its respective active list. The clearance active list can be tailored to each command. For example, the command may wish to monitor all users with a certain clearance level and can input these users into the Clearance Active List for this purpose.

In this example, there are designated active lists for each of these five indicator categories. This manually entered information serves as the "baseline" security characterization for that individual. Rules are applied against this base information to which rules are applied in order to evaluate in conjunction with any subsequent user events of security relevance. The example Foreign Influence Active List designed within ArcSight Express is shown in Figure 11:

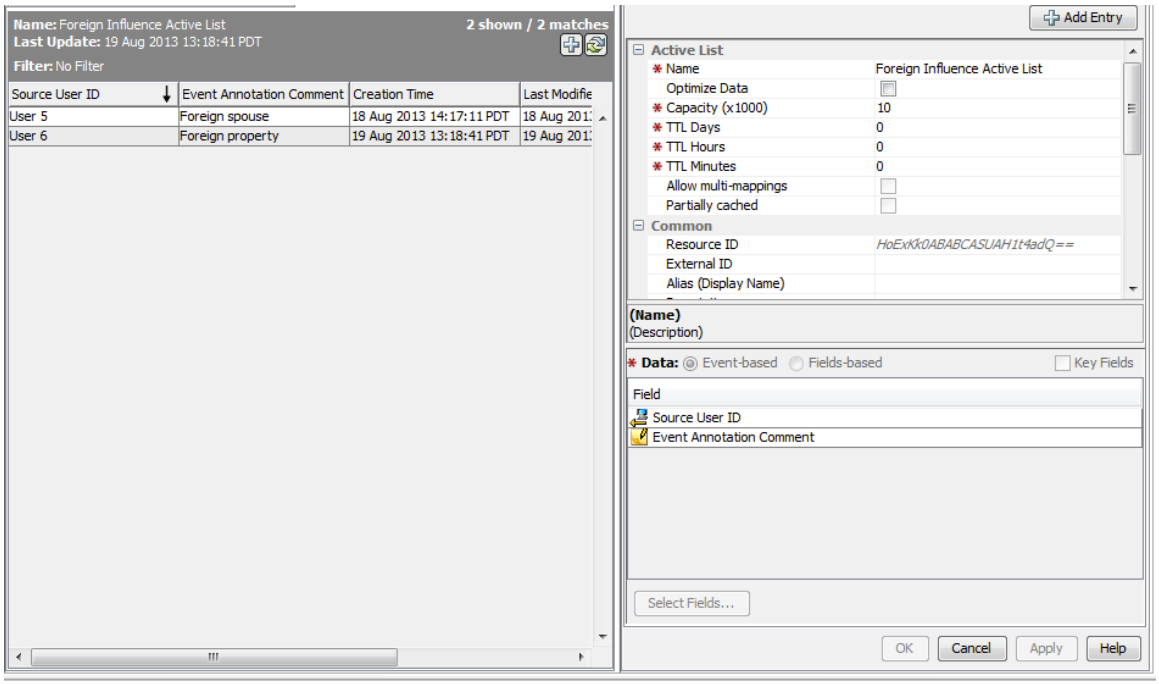


Figure 11. Foreign Influence Active List designed in ArcSight Express

The left side of the screenshot shows the content of the active list and the right side shows the characteristics of the active list. This list is updated manually. It shows the user IDs, in this case Users 5 and 6, and an inserted comment under the event annotation comment to describe the type of foreign influence: foreign spouse and foreign property in these examples. These manually updated active lists are designed with a time to live (TTL) of 0 in the time fields, which instructs the system to never expire them. These lists will then be used as conditions in various "insider" rules in order to assist the SIEM in focusing on specific users for potential malicious insider activities. The inclusion of the clearance level active list allows for commands to provide additional focus on individuals with certain clearance levels who may or may not have entries in the Foreign Influence, Financial, Disgruntlement, or Previous Arrest Active Lists.

The "dynamic" section of the design shown in Figure 10 includes the various log sources that will be used as basic inputs for the SIEM design. These log sources are based on the potential data exfiltration methods described in Chapter VI and include printers, e-mail activities, and web activities. These log sources are samples of the many potential log sources that can be implemented using this architecture as a basic template. Other log

sources can be implemented depending upon the structure of the specific command and its network components. In order for the SIEM to effectively process these log sources, filters must be used to eliminate designated normal activities for those nodes. The following paragraphs will describe examples of some of the conditions for the filters that can compose this architecture.

1. Data Exfiltration Filter

The components of this filter can be designed in ArcSight Express to include activities such as afterhours printing, excessive printer use, and e-mail characteristics such as time and size (Holloway & Santiago, 2012). As discussed in Chapter VI, these are potential means to exfiltrate data without proper authorization. The above described filters can be incorporated, in conjunction with a login active list, into rules that evaluate these conditions and provide input to a related active list. An example data exfiltration filter concerning printer events is shown below in Figure 12. This filter allows events through that meet the conditions defined in the filter. Some possible conditions, as shown in Figure 12, could be files sent to the printer larger than 1 megabyte, or sent between the hours of 1700 and 0600. These events may require further analysis. These times and file sizes can be adjusted to values based on specific command requirements. For example, some users at a command may consistently work after hours or send large files causing potential false-positives. Establishing baseline behavior would assist the command in fine-tuning this filter and perhaps even developing filters for each user based on their typical network activities. The values used here simply provide an example of a filter's capabilities for use in the overall SIEM architecture.

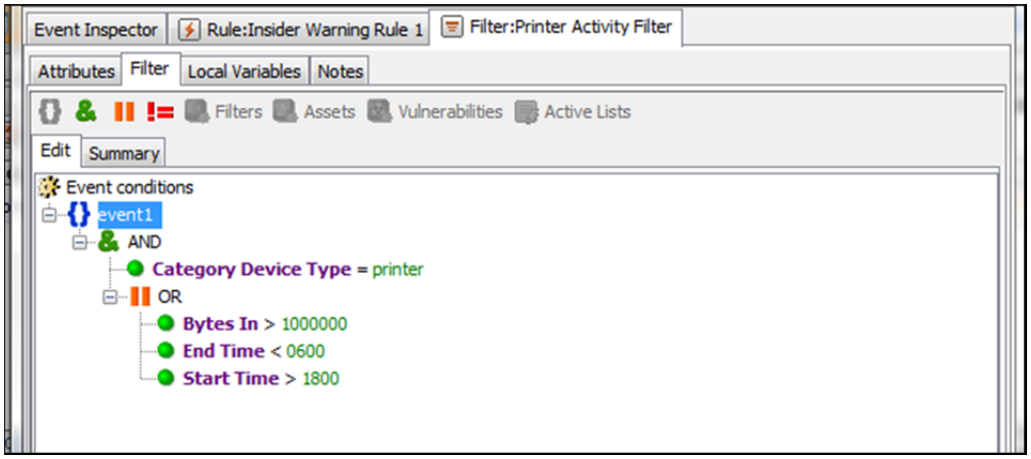


Figure 12. Printer conditions for data exfiltration filter (After Holloway & Santiago, 2012)

2. Financial Filter

These financial filters can be designed in ArcSight Express to focus on user Web activity. Specifically, these filters focus on user visits to pre-designated websites that may indicate potential financial issues for the individual. For example, major bankruptcy websites can be entered into the filter as a condition. Also, the filter can be designed to include key words within the URL visited. If a user visits one of these pre-designated or key word websites, then that event will be included in the filter and the filter can then be used as a condition in a rule. A user visiting these sites may be indicative of potential financial issues. This filter would also typically contain specified information to designate the log source, such as asset id, or category group, in order to further define the specific logs as sources for this filter (Holloway & Santiago, 2012).

3. Foreign Influence Filter

This filter can be designed to specifically look for any Web surfing activity to non- .mil, .gov, .com, .org, or .edu domains. This filter records activity to domains outside of those typically used for work-related functions. This filter can also include e-mails sent to these domains (Holloway and Santiago, 2012). For example, if an individual has a previous background condition indicating potential foreign influence from Russia,

visits or e-mails to a .ru domain might be reason for further investigation, and this filter will provide the event information for further evaluation.

4. User Login Rule

The user login rule includes the log sources of designated operating systems and writes the user ID and time of access to an active list. This active list contains an expiration time of one day as it will be refreshed each day. This active list containing the user IDs, system IDs, and times of access can then be used as a condition for three rules: the financial rule, the foreign influence rule, and the data exfiltration rule. These three rules take the previously described filters and relate them to the user IDs contained within the User Login Active List.

5. Financial, Foreign Influence, and Data Exfiltration Rules

The financial rule takes the associated financial filters and compares them to the User Login Active List. If there is a user logged in and the user ID matches with one of the filters, then the user ID information is output to the Financial Activity Active List. An example of the financial rule is shown in Figure 13:

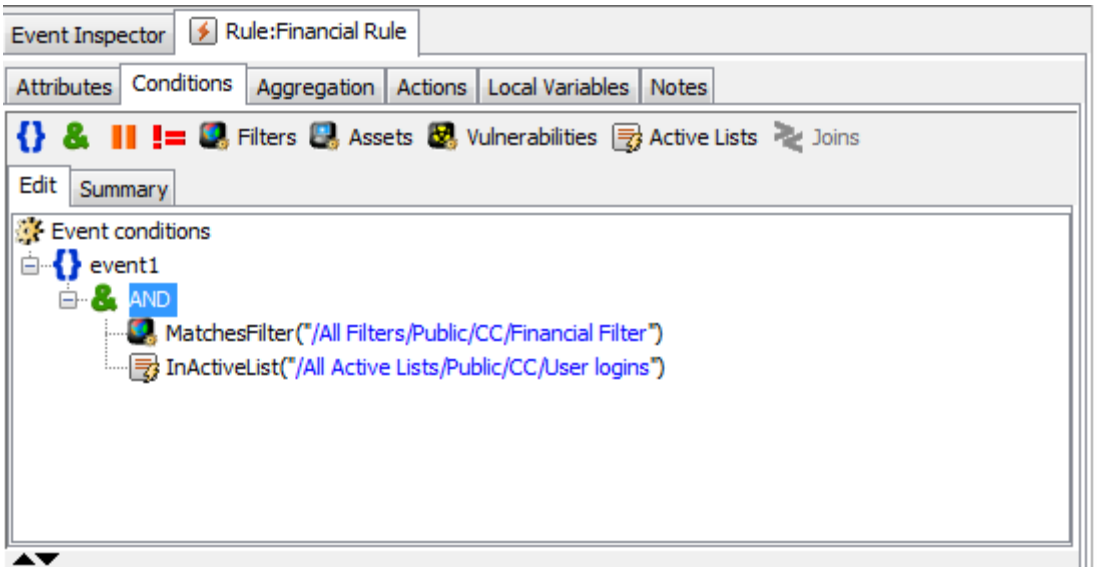


Figure 13. Financial rule designed using ArcSight Express

The rule shown in Figure 13 evaluates both the financial filter condition and the User Login Active List condition. If the user ID is present in both of these conditions, the rule will output to the Financial Activity Active List. Figure 14 shows the screen defining the rule actions. This rule outputs the Source User ID based on its occurrence in both the financial filter and the User Login Active List to the Financial Activity Active List for each event.

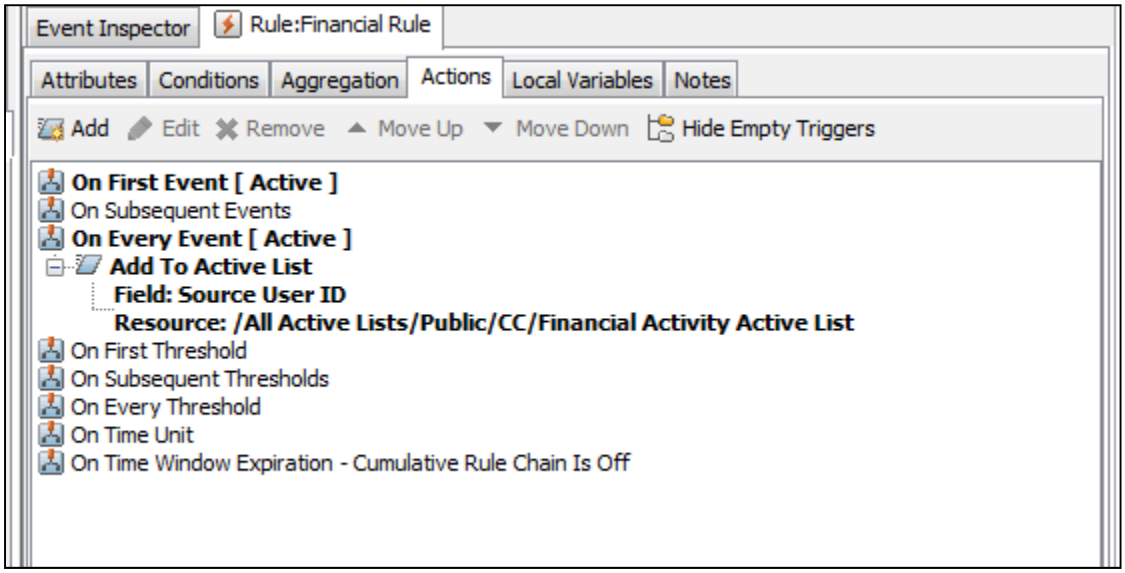


Figure 14. Financial rule action designed using ArcSight Express

Each of these activity rules will output to a specified active list as shown in Figure 10. These active lists will then be used as conditions for evaluation by the Insider Warning rules.

6. Indications and Insider Warning Rules

There are two rules within this section of the architecture shown in Figure 10. The first rule, the Indications rule, takes the three active lists underneath the dynamic section of Figure 10 and compares them with the user Foreign Influence Active List, User Financial Active List, Disgruntlement Active List, and Previous Arrest Active List. If a user ID is NOT on at least one of these four active lists, but IS on one of the activity

active lists, then that user ID is added to the Indications Active List as shown in Figures 15 and 16.

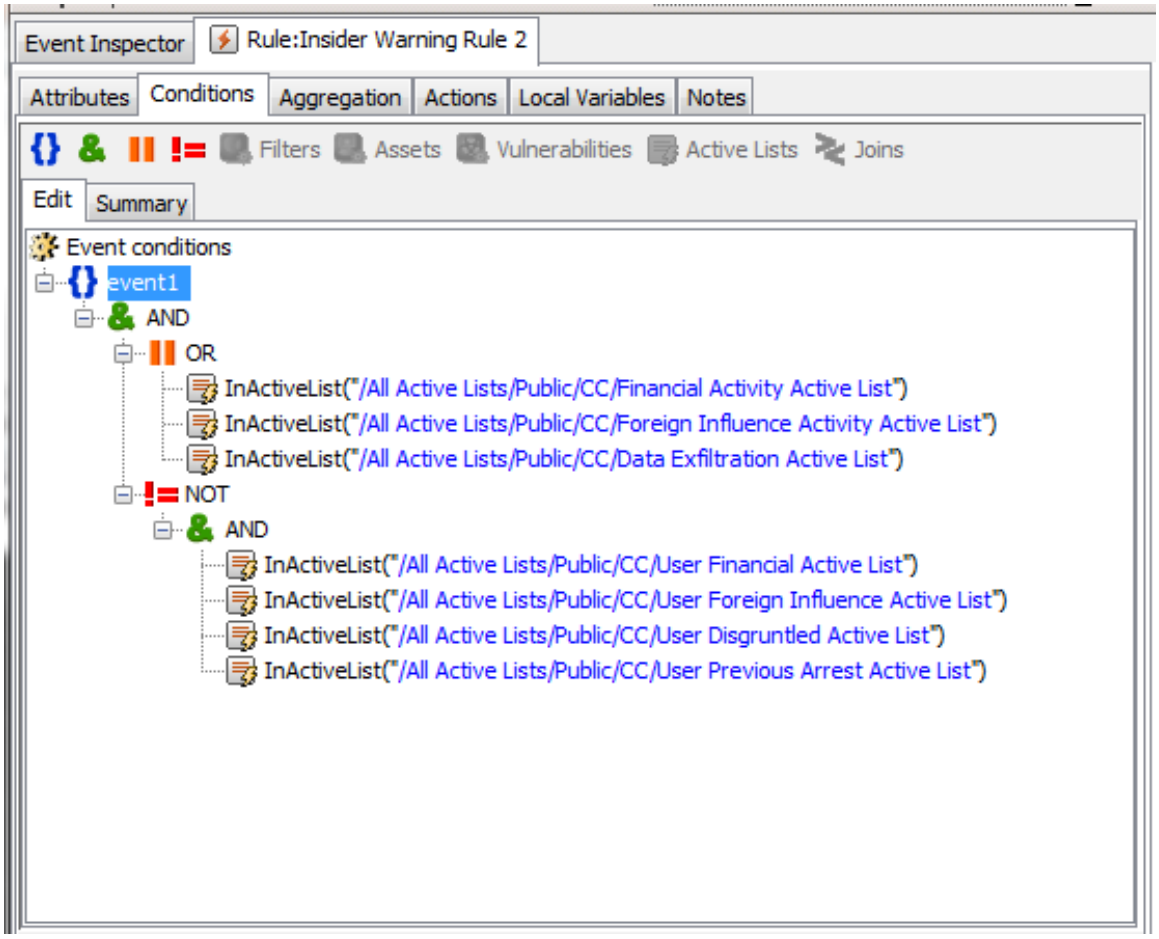


Figure 15. Indications rule designed using ArcSight Express

The rule shown in Figure 15 states that if a user ID is in the Financial Activity Active List, OR the Foreign Influence Activity Active List, OR the Data Exfiltration Active List; AND the user ID is NOT in one of the four manually developed User active lists based on previous indicators, then the user ID will be output to the Indications Active List as shown in Figure 16. This rule does not include the Clearance Active List as this active list will be used as a condition within the second Insider Warning rule.

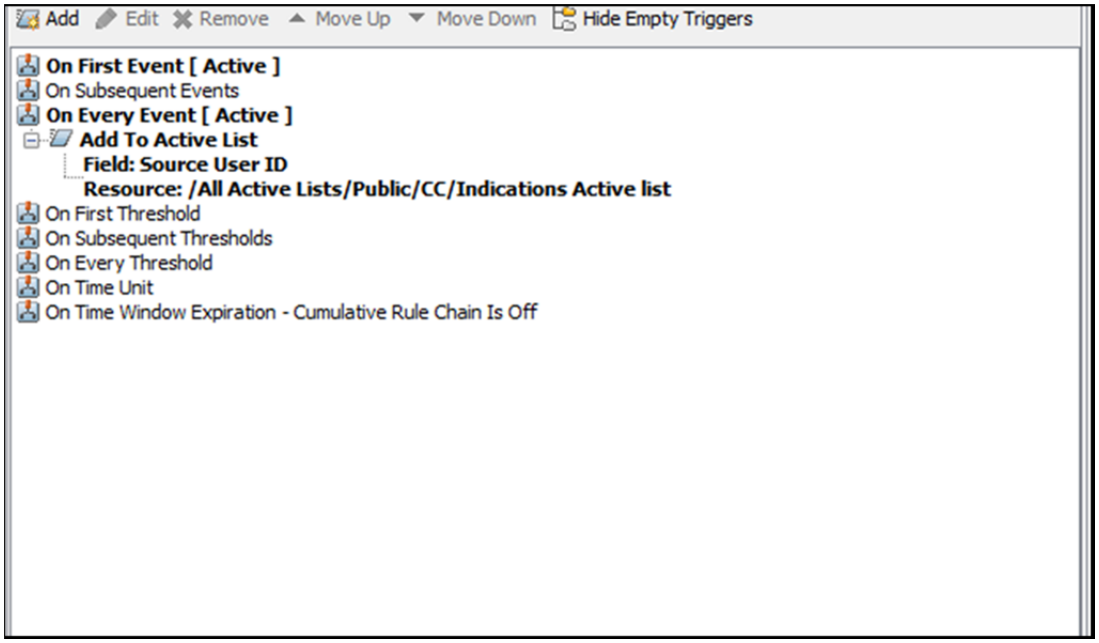


Figure 16. Indications rule output to Indications Active List designed using ArcSight Express

The reasoning for this indications rule is to capture activity by users who may not have previous indicators on their record from their PSI and administrative action history. This provides another possibility for evaluation by designated personnel to capture activity by individuals who were not already on one of the manually entered active lists. The user ID must then be manually added to its respective User active list depending on the type of event activity (financial, foreign, or data exfiltration). Once these events are added to their respective user active lists, appropriate information can then be captured and evaluated (along with other event conditions) using the Insider Warning rule as shown in Figure 17.

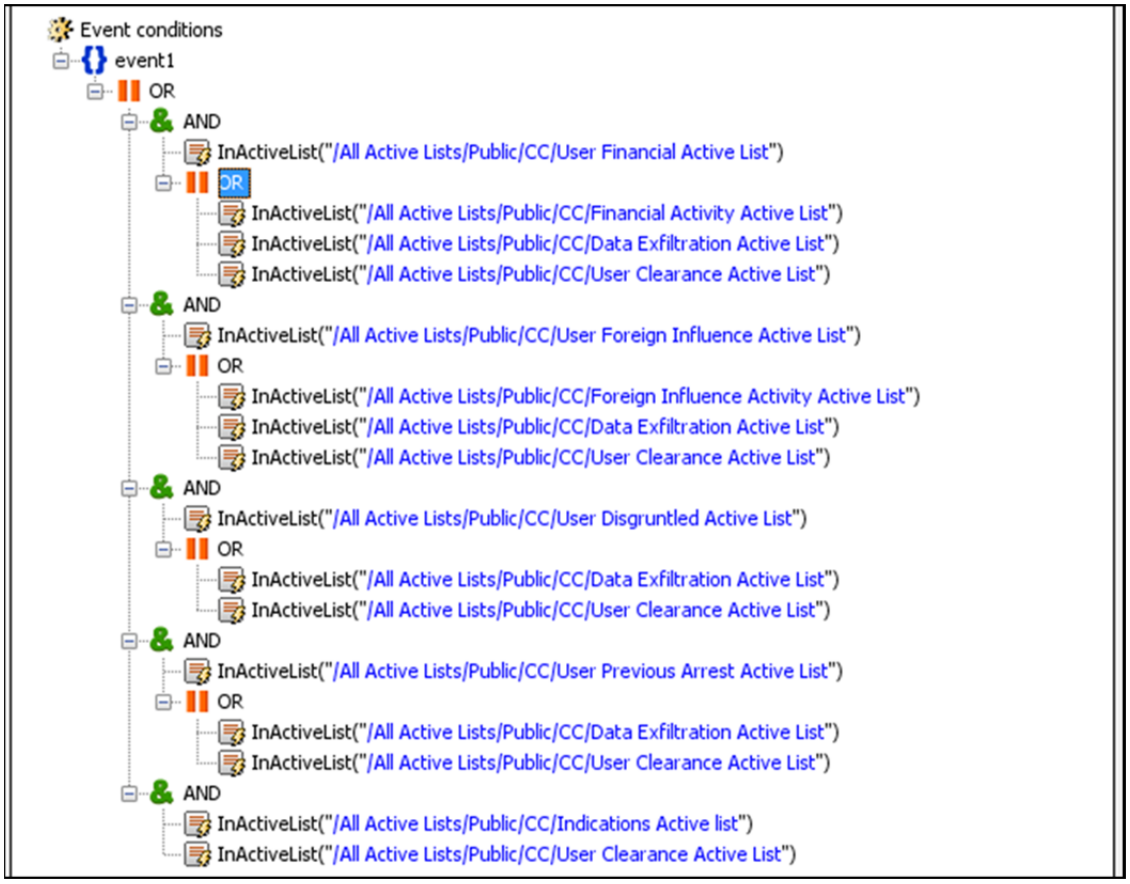


Figure 17. Insider Warning rule designed using ArcSight Express

The Insider Warning rule shown in Figure 17 contains five sections. The first logical operator used is "OR." If an event matches the first sub-conditions within the rule OR the second OR the third OR the fourth OR the fifth; then the rule action will be to write the user ID to the Insider Warning Active List.

The first section of the Insider Warning rule begins with the AND logical operator. If a user ID is in the User Financial Active List AND the user ID is either in the Financial Activity Active List OR the Data Exfiltration Active List OR the Clearance Active List; then this satisfies the condition for the rule and the user ID will be added to the Insider Warning Active List. The reasoning behind this rule segment is that if an individual is already on an active list based on their PSI or administrative action entries for any type of financial issues and the user ID shows up on the current Financial Activity Active List, this should be added to a warning list for further evaluation. Also, if the user

is on the User Financial Active List AND shows up on the Data Exfiltration Active List, this also might be an event that requires further evaluation and the user ID will be added to the Insider Warning Active List. Finally, if the user ID is on the User Financial Active List AND has the specified clearance level designated on the User Clearance Active List, then the user will be added to the Insider Warning Active List. This allows a command to capture potential activities by individuals who hold certain clearance levels. For example, individuals with higher clearance levels may be able to cause more damage. Thus the command may want to capture suspect activities using this format. The reasoning is the same for the construction of the second sub-condition related to foreign influence.

For the third and fourth sections of the Insider Warningrule, if the user ID is on the User Disgruntled Active List AND is on the Data Exfiltration Active List OR the Clearance Active List, this indicates an event requiring further evaluation and will thus be added to the Insider Warning Active List. The same is true if the user ID is on the Previous Arrest Active List AND the Data Exfiltration Active List OR the Clearance Active List. For example, if a user is on the Clearance Active List and is later manually added to the Previous Arrest Active List for an incident during the user's time at the command (i.e., after initial check-in), this rule will evaluate the conditions and automatically add this user ID to the Insider Warning Active List based on his being on both the Previous Arrest AND Clearance Active Lists.

For the fifth section, if a user ID is added to the Indications Active List AND is on the Clearance Active List, this will also output to the Insider Warning Active List. The reasoning for this section is that a command will most likely want to monitor any suspicious events related to users with certain clearance levels, and these users may not have any previous background indicators in their records. This allows for further investigation as necessary.

By using previously formatted active lists as conditions to the Insider Warning rule, this allows management the flexibility to re-arrange and design the rule conditions to match their requirements. For example, a commanding officer, may desire to link the User Disgruntled Active List with the Financial Activity and Foreign Influence Active Lists for further monitoring of potential disgruntled user activities. This can be done by

simply re-arranging the logical operators and supplying the necessary active lists as conditions.

The rule in Figure 17 has outputs to the Insider Warning Active List, as shown in Figure 18.

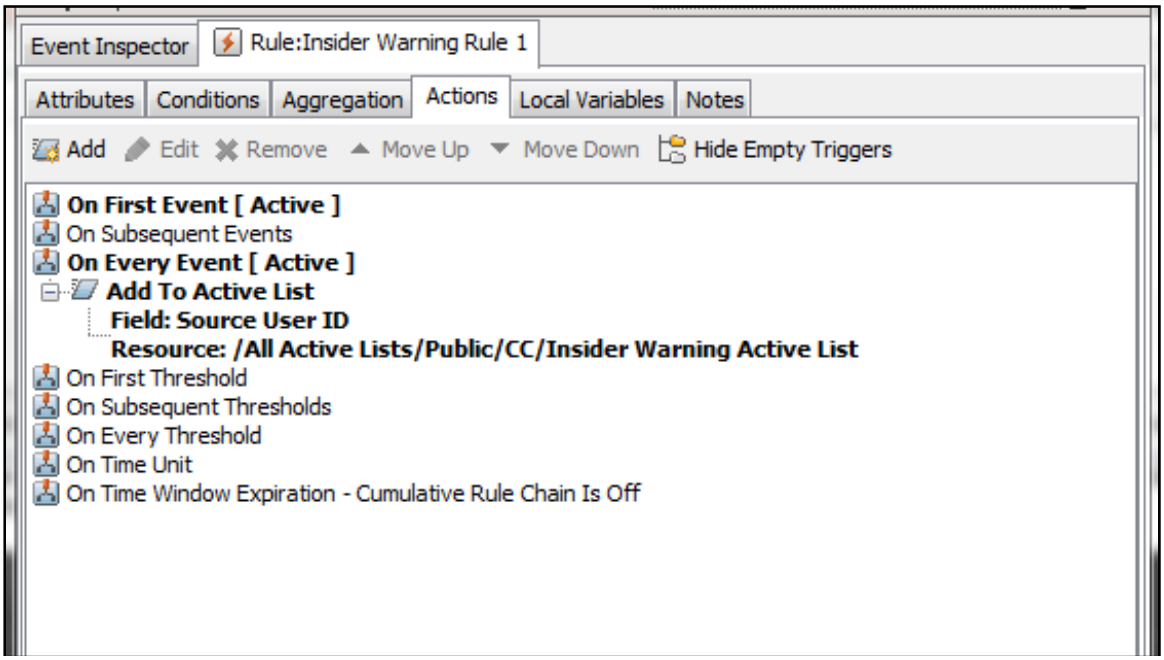


Figure 18. Insider Warning Rule output to Insider Warning Active List designed using ArcSight Express

For each event that matches one of the primary OR conditions of the Insider Warning rule, the user ID will be added to the Insider Warning Active List. The Insider Warning Active List will have a TTL of zero so that it can be reviewed at any time by designated personnel.

The use of two rules and active lists for this architecture as shown in Figure 10 provides a tiered structure for evaluation purposes. An individual showing up on the Indications active list may not warrant a detailed investigation, but a command may still want to record these activities and possibly investigate. However, if the individual shows up on the Indications Active List and has a clearance level of concern for the command,

the system automatically places them on the Insider Warning Active List. Also, if an individual has background indicators of concern, then the system will automatically add them to the Insider Warning Active List if their network activities drive them to placement on one of the Activity active lists and the specifics of the events can then be further evaluated.

User ID additions to the Indications or Insider Warning Active Lists do not prove that an individual conducted potential malicious insider activities, but it is a cue for further evaluation and can assist in the previously described goals of deterrence, prevention, and detection. By adding the user ID to these active lists based on these conditions, false positives will most likely occur at some point. User activity that results in their addition to these active lists could be simply part of their routine job activities or other benign situations. However, highlighting the user's name offers management the opportunity to investigate and determine whether or not this was simply a false positive or an actual event of concern. A command's response to false positives could be time consuming, however, a command's response to a false negative, where an actual malicious event occurred, is most likely much more resource intensive. For these reasons, this architecture using multiple, grouped active lists is designed to be more general in nature. By not having individual rules and individual active lists designed for each user, this means more non-malicious users will potentially trip one of the rules and require further action by the command to investigate innocent activities. However, this tips the false-indications balance in favor of too many false-positives rather than missed false-negatives.

This example SIEM architecture was used to illustrate the potential and flexibility associated with using the various components of a SIEM to detect or prevent insider threats. As previously described, these components can be arranged in a variety of ways to better meet specific command needs or requirements.

VIII. CONCLUSIONS AND FUTURE WORK

A. CONCLUSIONS

This thesis reviewed the basics of SIEMs, insider threats, Navy PSI and administrative actions and data exfiltration methods. The objective of this thesis was to show how Navy commands can potentially include PSI and administrative actions for individuals into a SIEM framework for purposes of deterring, preventing, and detecting insider threats.

This objective was satisfied through the architecture described in Chapter VII. A detailed process of including individuals' background information from their PSI and any administrative actions as input to a SIEM was described. This process uses multiple active lists to create rules based on user background data and their network activity that would trigger alerts of potential insider misuse. If a user conducts pre-defined suspicious network activity, then the user's ID is added to an active list for further investigation by designated command personnel. Additionally, this architecture allows a Navy command to focus on the network activities of users with certain clearances. The example architecture provided can serve as a basis for further evaluation for the potential benefits of using user background information as components of a SIEM to assist in combatting malicious insiders.

B. BENEFITS TO THE DON

Personnel with authorized access to Navy accounts and networks, combined with malicious intent, present a uniquely challenging threat that needs to be mitigated via deterrence, prevention and detection. Malicious insiders can pose a significant threat on CONUS networks, ships' networks, and forward-deployed networks. The research conducted for this thesis and the architecture described will potentially add capabilities for combating insider threats on Navy networks.

Even unclassified data can provide enemy forces with insight into Navy operations and intentions, violating operational security and putting U.S. forces and personnel at risk. Time gaps between security background investigations, combined with

not updating user profiles with any sort of administrative action, can increase the risk of insider threats.

The combination of personnel data already collected during the security clearance process with documented administrative actions, along with the network account accesses and activities, can give network administrators and commanding officer's better insight into their personnel's network activities. By using a SIEM tool to correlate user activity with their detailed account profile, the pre-defined rules can trigger alerts of potentially malicious activity based on specific events, and these can stimulate further investigations.

C. FUTURE WORK

There are some basic issues that will need to be researched and addressed prior to including a SIEM tool as a basic component of a command's insider threat program. The architecture described in Chapter VII uses basic filters, active lists and rules as its components. These filters can be further defined to capture even more relevant data based on a variety of log sources, producing even more active lists and potentially more rules. The components shown in Chapter VII were used to illustrate the potential of the tool and can be expanded to further enhance the abilities of this tool.

Purchase costs, administration, and training for the use and implementation of this tool also need to be considered. A cost-benefit analysis can assist in determining the feasibility of using this type of tool, quantifying the costs of the SIEM, maintenance, training, and administration against its ability to effectively combat insider threats. Additionally, the legalities of including an individual's PSI and administrative actions on a network access request form need to be addressed out of concern for privacy and possible Constitutional issues. Privacy issues would also need to be resolved in order for the JPAS process to be changed to allow specifics from the PSI readily accessible by security personnel for inclusion as SIEM sources.

Another aspect requiring future work is the transmission of the user information to travel with them from command to command. While the PSI and documented administrative actions will always be a component of the individual's record, regardless of location; the specific network activities recorded on the previously described active

lists will remain at that specific command. A means to incorporate these active lists into a user's record, accessible Navy-wide, could provide greater fidelity into the user's total activity across commands. Additionally, a method for a user's recorded network activities to be accessible across service boundaries would provide even further fidelity on an individual across their career. Automating the process by which SAAR-N information can be entered into the active lists may also be possible by using a cloud service. This would decrease the administrative burden of manually entering user information. Consideration and research of the above described items can further increase the effectiveness of using a SIEM tool against insider threats, increasing the overall security posture of the Navy's networks.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Amazon Web Services. (2013). *Amazon simple storage service (Amazon S3).* Retrieved from http://aws.amazon.com/s3/

ArcSight (2011, August). *ESM console user's guide: ArcSight express v3.0 featuring ESM with CORR engine storage*.

ArcSight (2012, January). *ESM 101: Concepts for ArcSight ESM v5.2*.

Capelli, D., Moore, A., & Trzeciak, R. (2012). *The CERT guide to insider threats*. Upper Saddle River, NJ: Addison-Wesley.

CERT. (2011, April). *Insider threat control: using a SIEM signature to detect potential precursors to IT sabotage.* Pittsburg, PA: Carnegie Mellon Software Engineering Institute. Retrieved from http://www.cert.org/insider_threat/

Chief of Naval Operations. (2011, July 11). Physical readiness program. Washington, DC: Author. Retrieved from http://www.navy-prt.com/files/6110.1J_-_Physical_Readiness_program.pdf

Contos, B. T. (2006). *Enemy at the water cooler*. Rockland, MA: Syngress Publishing.

Defense Personnel Security Research Center (2009, November 2). *Espionage and other compromises of national security*. Retrieved from http://www.dhra.mil/perserec/espionagecases/espionage_cases_august2009.pdf

Defense Personnel Security Research Center (2013, June 15). *Initiatives: Automated continuing evaluation System (ACES).* Retrieved from http://www.dhra.mil/perserec/currentinitiatives.html

Dempsey, K., Chawla, N., Johnson, A., Johnston, R., Jones, A., Orebaugh, A., Scholl, M., & Stine, K. (2011, September). *Information security continuous monitoring (ISCM) for federal information systems and organizations*. (NIST SP800–137). Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from http://csrc.nist.gov/publications/nistpubs/800–137/SP800–137-Final.pdf

Deputy Chief of Naval Personnel. (2009, October). *Naval military personnel manual, NAVPERS 15560D.* Millington, TN: Author. Retrieved from: http://www.public.navy.mil/bupers-npc/reference/milpersman/Documents/Whole%20MILPERSMAN.pdf

Hanley, M., & Montelibano, J. (2011, October). *Insider threat control: using centralized logging to detect data exfiltration near insider termination.* Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University. Retrieved from http://www.cert.org/archive/pdf/11tn024.pdf

Herbig, K. Northrop Grumman Technical Services (2008, March). *Changes in espionage by Americans: 1947–2007*. Retrieved from http://www.dhra.mil/perserec/reports/tr08–05.pdf

Holloway, R., & Santiago, E. (2012, August 13). *Understanding insider threats.* Palo Alto, CA: Hewlett-Packard. Retrieved from https://protect724.arcsight.com/docs/DOC-3019

Information Assurance Technology Analysis Center. (2000, April 24). *DoD insider threat mitigation*. Ft. Belvoir, VA: Defense Technical Information Center. Retrieved from http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA391380

Judge Advocate General. (2012, June 26). *Manual of the judge advocate general.* Washington DC: Author. Retrieved from http://www.jag.navy.mil/library/instructions.htm

Joint Personnel Adjudication System (JPAS). (2013, April 15). *JPAS frequently asked questions*. Retrieved from https://www.dmdc.osd.mil/psawebdocs/docRequest//filePathNm=PSA/appId=560/app_key_id=1559jsow24d/siteId=7/ediPnId=0/userId=public/fileNm=JPAS+General+FAQ.pdf

Keeney, M., Kowalski, E., Cappelli, D., Moore, A., Shimeall, T., & Rogers, S. (2005, May). *Insider Threat Study: Computer system sabotage in critical infrastructure sectors.* Pittsburgh, PA: Carnegie Mellon Software Engineering Institute & Washington, DC: United States Secret Service. Retrieved from http://www.cert.org/archive/pdf/insidercross051105.pdf

Kowalski, E., Conway, T., Keverline, S., Williams, M., Capelli, D., Willke, B., & Moore, A. (2008, January). *Insider threat study: illicit cyber activity in the government sector*. Pittsburgh, PA: Carnegie Mellon Software Engineering Institute & Washington, DC: United States Secret Service. Retrieved from http://www.cert.org/archive/pdf/insiderthreat_gov2008.pdf

Miller, D., Harris, S., Harper, A., VanDyke, S., & Blask, C. (2011). *Security information and event management (SIEM) implementation.* New York: McGraw Hill

Moore, A., Kowalski, E., & Cappelli, D. (2008, January). *Insider threat study: Illicit cyber activity in the information technology and telecommunications sector.* Pittsburgh, PA: Carnegie Mellon Software Engineering Institute & Washington, DC: United States Secret Service. Retrieved from http://www.cert.org/archive/pdf/insiderthreat_it2008.pdf

Nicolett, M., & Kavanagh, K. (2012, May 21). *Critical capabilities for security information and event management.* Stamford, CT: Gartner, Inc.

OPNAV 5239/14 (2011, September). *System authorization access request navy (SAAR-N).* Retrieved from: http://www.public.navy.mil/bupers-npc/enlisted/cmsid/Documents/SAAR-N_OPNAV_5239_14_Rev_9_2011.pdf

Randazzo, M., Keeney, M., Kowalski, E., Cappelli, D. & Moore, A. (2004, August). *Insider threat study: Illicit cyber activity in the banking and finance sector.* Pittsburgh, PA: Carnegie Mellon Software Engineering Institute & Washington, DC: United States Secret Service. http://www.cert.org/archive/pdf/bankfin040820.pdf

Secretary of the Navy. (2006, June). *DON personnel security program (SECNAV M-5510.30).* Washington, DC: N09N2 Retrieved from http://doni.daps.dla.mil/secnav%20manuals1/5510.30.pdf

Sensage. (n.d.) *A practical guide to next-generation SIEM.* Retrieved from http://www.sensage.com/sites/default/files/sens_gd_next-gen_siem_03ol.pdf. Last checked 2013, September 16.

Schultz, E. (2009). Security information and event management (SIEM) technology. In H.F. Tipton & M. Krause (Eds.), *Information Security Management Handbook,* Sixth Edition, Volume 3. New York: Isc2 Press.

U.S. Office of Personnel Management. (2010, December). *Standard form 86 (SF-86*): *Questionnaire for national security positions.* Retrieved from: *http://www.opm.gov/forms/pdf_fill/sf86.pdf*

Under Secretary of Defense (I). (2012, February 24). DoD information security program: controlled unclassified information. *DoD Manual 5200.01,* Volume 4. Washington, DC: Author.

Under Secretary of Defense (I). (2012, May 4) *Countering espionage, international terrorism and the counterintelligence (CI) insider threat (DoD Instruction 5240.26).* Washington, DC: Author.

Under Secretary of the Navy. (2013, February 27). *Personnel security investigation (PSI) reduction requirements.* Washington DC: Author. Retrieved from http://www.ncis.navy.mil/securitypolicy/Personnel/Personnel%20Security%20Policy%20%20Related%20Information/PSI%20Reduction%20Memo%202013%20(Signed).pdf

Weiss, P. (2013, May 2). *What you need to know about Bradley Manning.* Mondoweiss. Retrieved from http://mondoweiss.net/2013/05/should-bradley-manning.html

White House (2012, November 21). *National insider threat policy and minimum standards for executive branch insider threat programs.* Retrieved from http://www.whitehouse.gov/the-press-office/2012/11/21/presidential-memorandum-national-insider-threat-policy-and-minimum-stand

Naval Criminal Investigative Service (NCIS) Security Policy. Frequently Asked Questions. Retrieved from http://www.ncis.navy.mil/securitypolicy/FAQ/Pages/default.aspx. Last checked 2013, September 16.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California